

Filozofski fakultet
Odsjek za informacijske i komunikacijske znanosti
2013./2014.

Mladen Šlogar
Analiza percepcije informatike u popularnoj kulturi

Diplomski rad

Mentor: dr.sc. Vjera Lopina

Zagreb. 2014.

UVOD	5
1. RAZVOJ I PRISUTNOST INFORMATIKE	6
2. SPECIFIČNOST INFORMATIKE U POPULARNOJ KULTURI	6
3. INTERNET	7
3.1 Internetske usluge	7
Cloud computing	7
POP3 i IMAP protokoli.....	8
Rezerviranje avionskih karata.....	9
3.2 Internetski preglednici	9
Opera 9	9
Safari.....	10
Slimbrowser	10
3.3 Društvene mreže	10
Facebook	11
Tweeter	11
mySHOUT.....	12
3.4 Internetski pretraživači	12
Google	12
MSN Search i Bing	13
Finder-Spyder	13
Search-Wise.net.....	14
Roundsearch.....	14
3.5 Internetske stranice	15
Youtube.....	15
Craigslis t	15
Wikipedia.....	16
PayPal.....	16
Backgammon online.....	16
Soba za razgovor s računalnom sintezom govora	17
The Book World.....	17
Pohranjenost stranica na računalu	18
3.6. Računalne mreže	18
Network Address Translation.....	18
Apsolutna URL adresa	19
Podmreža.....	19
Proxy serveri	20

4. PROGRAMI	21
4.1. Sigurnosne snimke.....	21
Zapisi nadzornih kamera	21
Sigurnosne snimke i Windows Media Player	22
4.2. Računalne igre	23
Wolfenstein 3D	23
Left 4 Dead, Resident Evil 4 i Call of Duty – World at War.....	24
Igre kretnjom	25
4.3. Prepoznavanje lica	25
Biometrijska analiza	26
4.4. Programi za obradu slike.....	27
Photoshop	27
4.4.1. Programi za uvećavanje i izoštravanje slike.....	28
Realna primjena	28
Fiktivna primjena	29
4.5. Programi za prisluškivanje.....	30
Pro Tools.....	30
Program za transkripciju.....	31
5. RAČUNALNA SIGURNOST	32
5.1. Lozinke.....	32
Vidljivost lozinke	33
Najčešće korištene lozinke	33
Lozinka za tvorničke postavke.....	34
5.2. Kriptografska zaštita.....	34
Gibson & Joukowsky algoritam.....	35
AES.....	35
Vernamova šifra	36
5.3. Virusi.....	37
Cookie Monster	37
Rabbit virus	38
GPI i FSI virusi	38
Keystroke virus.....	39
5.4. Hidra	39
5.5. Snifferi.....	39
5.6. Botovi.....	40

5.7.	Back door	41
5.8.	Logička bomba i stražnja vrata	41
5.9.	Hardversko hakiranje	42
6.	HARDVER	43
6.1.	Dial-up.....	43
6.2.	Superračunala, William Gibson i <i>heavy metal</i>	44
6.3.	Oštećenje podataka	45
6.4.	Aktivna matrica.....	46
6.5.	Višestruki ekrani i DS3 veza	46
6.6.	28.8 bps modem i P6 procesori	47
6.7.	Kloniranje	48
7.	INFORMATIČKE REFERENCE	48
7.1.	Hakerski nadimci	49
7.2.	Savjest hakera	50
7.3.	Keyboard cowboy	50
7.4.	Zakon o računalnom kriminalu	50
7.5.	Charles Babbage	50
7.6.	2600.....	51
	ZAKLJUČAK	52

UVOD

U ovom radu pokušat ćemo proučiti na koji način je informatika prikazana u današnjoj popularnoj kulturi te koliko je taj prikaz vjerodostojan. Analizirat ćemo njene različite aspekte i pokušati ih objasniti. Među navedenima će biti prikaz Interneta, računalne sigurnosti i programa koji je omogućuju, razne programe koji se u uporabi te tehničke karakteristike računala koja su trenutno ili prije bila u uporabi. Također ćemo spomenuti reference na različita područja informatike i informatičke podrške koja se mogu pojaviti u raznim medijima.

Građi ćemo pokušati pristupiti objektivno bez obzira na način uporabe u mediju. Pronađeni materijali variraju po prisutnosti u medijima – programi mogu biti grafički prikazani ili samo opisani, a tehničke karakteristike računala mogu biti samo opisane ili i fizički prisutne u sadržaju. Također ćemo pristupiti građi bez obzira na opće znanje i prisutnost u popularnoj kulturi, tj. pristupit ćemo i manje poznatoj građi u slučaju njene prisutnosti u sadržaju.

Pokušat ćemo podijeliti proučenu građu u vjerno prikazane elemente i one koji nisu. U slučaju da je prisutna postojeća primjena informatike, ali je upotrijebljena u krivom kontekstu, bit će opisana i razjašnjena kriva uporaba. U slučaju nedovoljno razjašnjene uporabe termina, pretpostavit će se moguća uporaba u odnosu na kontekst radnje.

Također, prilikom analize moći ćemo primijetiti specifične odnose između informatike i njenom mjestu u popularnoj kulturi.

1. RAZVOJ I PRISUTNOST INFORMATIKE

Prilikom analize informatike u popularnoj kulturi bit će moguće usporediti njenu prisutnost u odnosu na razvoj računala tijekom 90-ih godina 20.-og stoljeća i na početku 21.-og stoljeća. Iako se nećemo isključivo posvetiti takvoj analizi zbog obujma analizirane građe, moći ćemo vidjeti na koji način se razvijala popularna kultura tijekom tog razdoblja.

Možemo pretpostaviti kako će prisutnost i primjena informatike u popularnoj kulturi biti proporcionalna razvoju računalstva. Rasprostranjenost informatike u svakodnevnom životu također će utjecati na njenu prisutnost u popularnoj kulturi, kao i sve veća uporaba osobnih računala s obzirom na proizvodnju novih tehnologija. To će nam omogućiti lakše shvaćanje načina na koji popularna kultura usvaja novu tehnologiju.

2. SPECIFIČNOST INFORMATIKE U POPULARNOJ KULTURI

U analizi građe također ćemo moći proučiti u kojoj vrsti materijala je moguća veća prisutnost stručne informatike u odnosu na više općenite primjere informatike. S obzirom na različitu tematiku proučenog sadržaja, specifičnost će varirati s obzirom na radnju i vrstu sadržaja.

Moguća pretpostavka je kako će prisutnost stručne informatike biti veća u žanrovima koji se primarno posvećuju računalstvu ili ovise o uporabi tehnologije za razvoj radnje. Uporaba informatike u svrhu povezanosti i komunikacije poput društvenih mreža također će vjerojatno ovisiti o žanru sadržaja, nužnosti za razvoj radnje, ali i o trenutnom razdoblju u kojem se radnja odvija. Razlog potonjeg je radi uzimanja u obzir razvoja računalstva i njegove primijenjenosti u društvu u navedenom razdoblju. Stoga možemo pretpostaviti kako postoji nekoliko mogućnosti koje treba uzeti u obzir analizirajući sadržaj.

3. INTERNET

Naglim širenjem pristupa tokom 1990-ih godina, Internet je postao jedan od glavnih izvora informacija i komunikacije te bitno sociološko i komercijalno središte današnjeg informacijskog doba. Za većinu današnjih aktivnosti koje zahtijevaju konstantan pristup informacijama Internet je postao nepohodno sredstvo. Na temelju proučene građe možemo zaključiti kako je njegova prisutnost zamijećena u skoro svakom obliku popularne kulture. Od filmova, serija, knjiga preko računalnih igara i pokretanja istih isključivo preko Interneta, on postaje svakodnevnom pojavom, kako u stvarnom životu, tako i u različitim oblicima popularne kulture. Na temelju građe percepciju Interneta možemo podijeliti na nekoliko kategorija i sukladno s njima analizirati na koji način je prisutan u proučenim medijima. Bitno je napomenuti kako je velika većina proučenog sadržaja nastala krajem 20.-tog i početkom 21.-og stoljeća zbog povećane dostupnosti Interneta.

3.1. Internetske usluge

Prilikom pristupa Internetu korisnici često upotrebljavaju različite usluge koje u načelu omogućuju lakše snalaženje i pristup podacima na Internetu. Prema analiziranoj građi možemo uočiti kako prevladava prikaz vjeran stvarnim protokolima i sustavima koji su danas u uporabi. Proučeni sadržaj se sastojao od serija i filmova različite tematike – od humorističnih i kriminalističkih serija čiji fokus nije tehnička preciznost preko trileru s primarnim fokusom na uporabu Interneta i računalne tehnologije u radnji. Možemo zaključiti kako proučeni primjeri ukazuju na opću osviještenost o funkcioniranju internetskih usluga. Neke od njih ćemo ovdje navesti.

Cloud computing

U američkoj humorističnoj seriji o zadatcima mjesne policije *Brooklyn Nine-Nine*, jedan od glavnih likova napomenuo je kako je njegov novi program za organizaciju rasporeda temeljen za „računalstvu u oblaku“ (engl. *Cloud computing*)¹. Računalstvo u oblaku je koncept u kojem lokalno računalo koje korisnik upotrebljava

¹ *Brooklyn Nine-Nine*: ep. 114 - 9.52min

nema više zadaću pokretanja svih aplikacija koje su krajnje nužne korisniku. Tu odgovornost preuzima „oblak“, tj. mreža računala koja ga sačinjavaju ². Zahvaljujući oblaku, korisnikova potreba za prikladnom hardverskom i softverskom podrškom postaje sve manja. Dakle, jedino što korisnik treba kako bi pristupio sustavu jest mogućnost pokretanja softverskog sučelja oblaka, dok umrežena računala obavljaju ostatak zadatka.

POP3 i IMAP protokoli

U epizodi britanske detektivske serije *Broadchurch* glavni istražitelj Alec Hardy djetetu koje je osumnjičeno za smrt svog prijatelja pokazuje ispis njegove elektroničke pošte. Na upit gdje su našli poruke, budući da je osumnjičenik uništio prijenosno računalo koje je upotrebljavao, detektiv objašnjava da su poruke bile pohranjene na serveru (hrv. poslužitelj), a ne na računalu ³. Prilikom slanja elektroničke pošte korisnikov klijent kojeg upotrebljava – npr. *Gmail* – povezuje se s *SMTP* serverom koji prosljeđuje sadržaj primatelju (engl. *Simple Mail Transfer Protocol*, hrv. protokol za jednostavno slanje pošte) ⁴. *SMTP* server može poslati poštu na jednu od dvije vrste servera s različitim protokolima. Kada korisnik namješta postavke svojeg korisničkog računa, mora odabrati vrstu protokola za server koji će njegov račun upotrebljavati. Mogući odabiri su *POP*, tj. *POP3* ili *IMAP*.

POP3, odnosno *Post Office Protocol 3* je protokol koji dolaznu poštu korisniku pohranjuje na tvrdom disku trenutnog računala koje korisnik upotrebljava. Prijašnje verzije *POP*-a su imale ograničenje u tome što su nakon pohranjivanja na računalu poruke bile izbrisane sa servera te im nije bilo moguće pristupiti s drugog računala ⁵. U tome je prednost *IMAP* protokola. *Internet Message Access Protocol* posjeduje mogućnost pregledavanja, ažuriranja i slaganja pošte bez potrebe za pohranjivanjem na računalo ⁶. Prema opisu pohrane sadržaja na serveru, možemo pretpostaviti da osumnjičenik u seriji upotrebljavao korisnički račun s *IMAP* protokolom, čime bi sva poslana i primljena pošta ostala pohranjena na *IMAP* serveru nakon što je policija dobila pristup računu.

² <http://computer.howstuffworks.com/cloud-computing/cloud-computing.htm>

³ *Broadchurch*: ep. 108 - 5.33min

⁴ <http://whatismyipaddress.com/mail-server>

⁵ <http://whatismyipaddress.com/pop3>

⁶ <http://whatismyipaddress.com/imap>

Rezerviranje avionskih karata

U američkom filmu *Mreža* Sandra Bullock tumači informatičkog analitičara Angelu Bennett. Pri početku filma Angela napravi rezervaciju avionske karte preko Interneta ⁷. Iako je danas takav način rezervacije sasvim uobičajen, 1995. godine kada je film i snimljen nije bila sasvim uobičajena pojava. Međutim, neke aviokompanije već tada nudile su takvu uslugu. Prva koja se mogla pohvaliti takvom inovacijom bila je američka aviokompanija *Alaska Airlines* te njena sestrinska tvrtka *Horizon Air*. Na službenim stranicama *Alaska Airlinesa* je navedeno kako su te dvije tvrtke bile prve američke aviokompanije koje su 1995. godine ponudile mogućnost rezerviranja i prodaje karata preko Interneta, iste godine kada je *Mreža* snimljena ⁸.

3.2. Internetski preglednici

Kako bi pristupili Internetu korisnici moraju upotrebljavati programe koji se zovu preglednicima. Oni omogućuju korisniku pristup Internetu i mogućnost njegovog pregledavanja. Proučeni materijali sastoje se od filmova serija koje se ne fokusiraju na računalnu tehnologiju i njenu uporabu, ali prikazuju preglednike radi razvijanja radnje. Uočena je uporaba stvarnih internetskih preglednika, uključujući i nekih manje poznatih. Razlog prikaza stvarnih preglednika može biti zbog njihove prepoznatljivosti kod većine gledatelja, ali i u svrhu njihovog oglašavanja.

Opera 9

U epizodi američke serije *Put prema dolje* jedan od glavnih likova pristupa Internetu preko internetsko preglednika *Opera* ⁹. *Opera* je stvari preglednik norveškog podrijetla dizajniran kako bi bio pouzdan i brz, kako na računalima, tako i na drugim platformama poput mobilnih uređaja. Preglednik podržava nekoliko operativnih sustava kao što su *Windows*, *OS X*, *Linux*, *iOS* i *Android* ¹⁰. Prema dizajnu preglednika u navedenoj epizodi, može se pretpostaviti da je riječ o devetoj

⁷ *Mreža*: 10.22min

⁸ <http://www.alaskaair.com/content/about-us/newsroom/technology.aspx>

⁹ *Put prema dolje*: ep. 212 - 19.20min

¹⁰ <http://www.operasoftware.com/company>

verziji preglednika zbog tada nove podrške za *widgete* čiji se izbornik može vidjeti u prizoru iz epizode ¹¹.

Safari

U američkom filmu *Kick-Ass 2* o sukobu superjunaka i superzlikovaca u stvarnom svijetu glavni negativac pretražuje Internet preko internetskog preglednika *Safari* ¹². *Safari* je stvarni internetski preglednik kojeg je razvila tvrtka *Apple* 2003. godine. Dok su u prošlosti upotrebljavali *Netscape* ili *Internet Explorer*, *Safari* je u travnju 2005. godine postao osnovni internetski preglednik kojeg upotrebljavaju računala *Appleove* proizvodnje ¹³. Prema izgledu i dizajnu preglednika, može se pretpostaviti da je verzija preglednika koja je prisutna u filmu *Safari 6* ili novija ¹⁴.

Slimbrowser

U epizodi serije *Put prema dolje*, jedan od glavnih likova čita članke na Internetu preko *Slimbrowsera* ¹⁵. *Slimbrowser* je stvarni nezavisni internetski preglednik tvrtke *FlashPeak*. Preglednik posjeduje mnoštvo unaprijed ugrađenih mogućnosti, kao što je blokiranje reklama, automatsko prevođenje internetskih stranica, skrivanje otvorenih stranica i mogućnost brze pretrage različitim pretraživačima ¹⁶.

3.3. Društvene mreže

Jedna od svakodnevnih pojava na Internetu su društvene mreže koje omogućuju povezanost svojih korisnika bez obzira na njihovu lokaciju. Jedini preduvjet je mogućnost pristupa Internetu. U proučenoj građi zamijetili smo prisutnost

¹¹ http://news.cnet.com/Opera-preview-puts-widgets-on-stage/2100-1032_3-6035227.html

¹² *Kick-Ass 2*: 19.30min

¹³ http://www.w3schools.com/browsers/browsers_safari.asp

¹⁴ http://www.macworld.com/article/1168043/safari_6_a_slight_but_sleek_upgrade_for_apple_s_browser.html

¹⁵ *Put prema dolje*: ep. 501 - 23.28min

¹⁶ <http://www.slimbrowser.net/en/webhelp/index.htm>

stvarnih društvenih mreža, ali i izmišljenih za potrebe serije. Primjeri ukazuju na medije u kojima računalna tehnologija nije fokus radnje. Unatoč tome primjeri su u većini slučajeva precizni i vjerno prikazuju stvarne mreže, dok fiktivni primjeri svojim dizajnom asociraju na funkcije i potrebe stvarnih društvenih mreža.

Facebook

Prilikom pretraživanja Interneta, glavni lik filma *Kick-Ass 2* proučava internetski profil jednog korisnika *Facebooka* ¹⁷. *Facebook* je trenutno najpopularnija besplatna društvena mreža na Internetu. Omogućava prijavljenim korisnicima stvaranje osobnih profila na kojima mogu postavljati vlastite slike i video sadržaj, slati poruke i stupati u kontakt s prijateljima, obitelji i kolegama. *Facebook* je dostupan na 37 jezika te omogućuje uređivanje profila po ukusu korisnika, kao i različite razine privatnosti kojima je moguće odrediti tko može vidjeti i pregledavati korisnikov profil ¹⁸.

Tweeter

U američkoj humorističnoj seriji *Parks and Recreation* o Sektoru parkova i javnih površina jedan od likova upotrebljava društvenu mrežu *twitter* ¹⁹, u seriji *Broadchurch* prikazano kako novinar ažurira svoje statuse na istoj mreži ²⁰, a u filmu *Kick-Ass 2* jedan od likova spominje uporabu *twittera* ²¹.

Twitter je pokrenut 2006. godine i glavna namjena usluge je za brzo širenje i nalaženje informacija. Usluzi je moguće pristupiti preko računala ili preko mobilnog uređaja u svrhu objavljivanja kratkih informacija u obliku *tweetova*, tj. sažetih poruka duljine do 140 znakova koje bilo tko može slati. *Tweetove* može čitati bilo tko, tko prati profil osobe koja ih je prva objavila ²².

U epizodi *Parks and Recreationa* glavni lik također spominje *hashtagove*. *Hashtag* je termin označavanja u društvenim mrežama kojim se mogu označiti

¹⁷ *Kick-Ass 2*: 19.30min

¹⁸ <http://whatis.techtarget.com/definition/Facebook>

¹⁹ *Parks and Recreation*: ep. 605 - 13.19min

²⁰ *Broadchurch*: ep. 101 - 30.56min

²¹ *Kick-Ass 2*: 23.10min

²² <http://socialmediatoday.com/daniel-zeevi/1371811/twitter-101-what-twitter-really-about>

ključne riječi unutar poruke radi lakšeg pretraživanja. Ključne riječi se označava simbolom za brojeve „#“. Ista funkcija je uvedena i u društvenu mrežu *Facebook* ²³.

mySHOUT

Na početku serije *Put prema dolje* Skyler White – jedan od glavnih likova – tražeći informacije o drugom liku otkriva njegov korisnički profil društvene mreže *mySHOUT* ²⁴. *mySHOUT* je fiktivna društvena mreža stvorena za potrebe serije ²⁵. Iako postoji *MYSHOUT* aplikacija za mobilne uređaje, društvena mreža iz serije nema nikakvu povezanost s njome ²⁶. Mreža je najvjerojatnije aluzija na stvarnu društvenu mrežu *myspace*. U doba emitiranja navedene epizode *Put prema dolje* 2008. godine, *myspace* je bila najposjećenija društvena mreža u svijetu s 75.9 milijuna posjetitelja mjesečno. Međutim, ubrzo je počela padati popularnost *myspacea* pojavom i razvijanjem *Facebooka* i *Twittera* ²⁷.

3.4. Internetski pretraživači

Kako bi našli željeni sadržaj na Internetu, korisnici načešće upotrebljavaju pretraživače koji na temelju unesenih riječi traže stranice sa sadržajem koji odgovara opisu. Uz postojeće pretraživače, moguće je uočiti i fiktivne verzije. Zbog različitih razloga možemo zaključiti kako je uporaba stvarnih i izmišljenih pretraživača podjednaka. S obzirom da se proučeni sadržaj uglavnom ne posvećuje tehničkog preciznosti, rezultati variraju.

Google

U britanskom filmu *Casino Royale* o pustolovinama tajnog agenta Jamesa Bonda glavni lik pretražuje Internet pomoću *Googlea* ²⁸. *Google* je poznat kao najpopularniji i najveći pretraživač te jedna od najpopularnijih internetskih stranica u

²³ <http://www.socialbakers.com/blog/1826-everything-you-need-to-know-about-hashtags-on-facebook>

²⁴ *Put prema dolje*: ep. 102 - 14.46min

²⁵ http://media.amctv.com/img/originals/breakingbad/myshout/pinkman_page.html

²⁶ <http://www.myshout.com.au/#shouthappy>

²⁷ http://www.businessweek.com/magazine/content/11_27/b4235053917570.htm

²⁸ *Casino Royale*: 45.32min

svijetu. Usluga korištenja pretraživača je besplatna, zahvaljujući proizvodima koji se reklamiraju nenametljivim poveznicama prilikom korištenja *Googleovih* usluga ²⁹.

U prvoj epizodi serije *Broadchurch* sestra ubijenog dječaka objašnjava kako ima namještene postavke u *Google Alertu* za riječi „*Broadchurch*“ i „smrt“ ³⁰. *Google Alert* je usluga koja stvara rezultate na temelju kriterija koje korisnik odredi. Dobiveni rezultati šalju se korisniku na račun njegove elektroničke pošte za daljnji pregled ³¹. Kao što je prikazano u seriji, usluga je korisna za pregledavanje specifičnih informacija na Internetu.

MSN Search i Bing

U epizodi američke kriminalističke serije *Žica* dva lika pretražuju Internet pomoću internetskog pretraživača *MSN Search* ³². *MSN Search* je pretraživač u vlasništvu američke tvrtke *Microsoft* ³³. 2009. godine pretraživač je zamijenjen novijom varijantom pretraživača koja se zove *Bing*. Za razliku od *MSN Searcha* koji je bio opisan kao „program za pretraživanje“ (engl. *search engine*), *Bing* je opisan kao „program za odlučivanje“ (engl. *decision-engine*) ³⁴. U filmu *Izvorni kod* iz 2011. godine glavni lik pretražuje pojmove na Internetu pomoću *Binga*, kao i glavni lik filma *Čudesni Spider-Man* iz 2012. godine ^{35 36}.

Finder-Spyder

U epizodi serije *Put prema dolje* *Skyler White* traži podatke o *Jesseju Pinkmanu* pomoću pretraživača *Finder-Spyder* ³⁷. *Finder-Spyder* je izmišljeni internetski pretraživač koji je korišten u neolicini američkih serija. Osim *Putu prema dolje*, upotrijebljen je i u *Zločinačkim umovima*, *Ekipi za očevid* i *Zakonu braće*.

²⁹ <http://google.about.com/od/googlebasics/p/whatisgoogle.htm>

³⁰ *Broadchurch*: ep. 101 - 32.45min

³¹ <http://www.wikihow.com/Use-Google-Alerts>

³² *Žica*: ep. 205 - 45.20min

³³ http://websearch.about.com/od/enginesanddirectories/a/msn_search.htm

³⁴ http://askbobrankin.com/what_is_bing.html

³⁵ *Izvorni kod*: 45.27min

³⁶ *Čudesni Spider-Man*: 14.00min

³⁷ *Put prema dolje*: ep. 102 - 14.22min

Najčešće se koristi kad nisu u mogućnosti upotrijebiti stvarne internetske preglednike poput *Googlea*, najvjerojatnije kako ne bi došlo do kršenja autorskih prava ³⁸.

Search-Wise.net

U britanskoj znanstveno-fantastičnoj seriji *Doktor Who* Rose Tyler upotrebljava internetski pretraživač *Search-Wise.net* kako bi otkrila tko je Doktor ³⁹. Internetska stranica za pretraživač postoji na Internetu i moguće joj je pristupiti, ali nije moguće pretraživati pomoću nje ⁴⁰. Pretraživač je dizajniran za potrebe serije ako se likovi trebaju koristiti internetskim pretraživačem u seriji .

Razlog fiktivnosti stranice je to što je serija u vlasništvu britanske javne televizije *BBC* koja ne dopušta reklamiranje stvarnih proizvoda i usluga poput *Googlea*. Korisnici *BBC-a* u Ujedinjenom Kraljevstvu plaćaju licencu kako bi mogli gledati i slušati sadržaj *BBC-a* bez oglašavanja, a i samo uredništvo *BBC-a* ima pravilnik kojim se ne dopušta uporaba *BBC-a* u svrhu reklamiranja komercijalnih proizvoda. Stoga je bilo nužno stvoriti izmišljenu verziju pretraživača za seriju ⁴¹ ⁴².

Roundsearch

U američkoj seriji *Sinovi anarhije* o životu motociklističkog kluba jedan od njegovih članova pokušava pomoću pretraživača naći dodatne informacije o izrazu „Meineke“ ⁴³. Može se vidjeti kako upotrebljava pretraživač *Roundsearch*. *Roundsearch* je izmišljeni internetski pretraživač koji je prvi put upotrijebljen u seriji „Američka horor priča“ te kasnije u *Sinovima anarhije* ⁴⁴. Budući da su obje serije u vlasništvu američke mreže *FX*, razumljiva je prisutnost pretraživača u oba slučaja ⁴⁵.

³⁸ <http://www.techrepublic.com/blog/geekend/geek-trivia-search-party-of-the-second-part/2/>

³⁹ *Doktor Who*: ep. 101 - 17.55min

⁴⁰ <http://search-wise.net/>

⁴¹ <http://www.bbc.co.uk/editorialguidelines/page/guidelines-editorial-integrity-advertising/>

⁴² <http://www.bbc.co.uk/bbc.com/faq/>

⁴³ *Sinovi anarhije*: ep. 106 - 16.28min

⁴⁴ <http://www.vulture.com/2011/12/websites-tv-made-up-this-year.html>

⁴⁵ <http://www.fxnowcanada.ca/shows/>

3.5. Internetske stranice

U većini sadržaja koji prikazuju uporabu Interneta moguće je vidjeti stranice koje likovi pregledavaju na Internetu. Iako ima i stvarnih primjera, zbog potrebe radnje neke stranice su najvjerojatnije izmišljene. Većina proučene građe upotrebljava različite stranice više zbog razvijanja radnje nego vjernog prikaza pregledavanja Interneta. Navedeni primjeri dakle prikazuju stvarne, odnosno fiktivne stranice ovisno jesu li prikladne za potrebe medija ili ne, iako prevladavaju stvarni primjeri zbog njihove popularnosti za specifične potrebe i usluge.

Youtube

U filmu *Skyfall* prikazana je uporaba internetske stranice *Youtube* ⁴⁶. U seriji *Put* prema dolje i filmu *Kick-Ass 2* likovi spominju uporabu navedene stranice ^{47 48}. *Youtube* je stvarna stranica za razmjenu video sadržaja preko Interneta. Osnovana je 2005. godine te je od 2006. u vlasništvu *Googlea*. Prednost stranice je u činjenici da većina video zapisa zauzima previše prostora za praktično slanje preko elektroničke pošte, stoga je moguće podijeliti zapis pohranom na *Youtubeu* i slanjem URL poveznice drugim korisnicima na Internetu. Osim pohrane privatnog sadržaja, *Youtube* koriste i različite tvrtke i interesne skupine za reklamiranje svojih proizvoda i usluga ⁴⁹.

Craigslist

Jonathan Ames – glavni lik humoristične serije *Ubi me dosada* – oglašava svoje usluge privatnog detektiva na internetskoj stranici *craigslist* ⁵⁰. *Craigslist* je stranica za oglašavanje te jedna od najposjećenijih stranica na engleskom jeziku. Svrha stranice je oglašavanje svih vrsta, od nekretnina, proizvoda, usluga i poslova. Izgled stranice je minimalistički, s jednostavnim, gotovo spartanskim, dizajnom i korisnim pretraživačem za lakšu navigaciju među oglasima. Zbog relativno malog

⁴⁶ *Skyfall*: 51.15min

⁴⁷ *Put* prema dolje: ep. 515 - 37.46min

⁴⁸ *Kick-Ass 2*: 20.52min

⁴⁹ <http://digitalunite.com/guides/tv-video/what-youtube>

⁵⁰ *Ubi me dosada*: ep. 101 - 4.22min

broja zaposlenih, većinu oglasa pregledavaju i uređuju sami korisnici *craigslista*. Iako je započeta samo s oglasima u području San Francisca, *craigslist* danas pokriva oglašavanje mnoštva američkih gradova, ali i europskih, uključujući i hrvatskih ⁵¹.

Wikipedia

U Putu prema dolje Skyler pregledava članke o pranju novca na internetskoj stranici *Wikipediji* ⁵². *Wikipedia* je besplatna enciklopedija koja omogućava registriranim korisnicima kreiranje novih članaka, dok za uređivanje članaka nije potrebna prijava. Stranicu su osnovali Jimmy Wales i Larry Sanger u siječnju 2001. godine kao stranicu koja bi podržavala *Nupediu*. S vremenom je *Wikipedia* postala veća od *Nupedie* te je time trenutno jedna od najpopularnijih internetskih stranica u svijetu ⁵³.

PayPal

Walter White mlađi, jedan od glavnih likova Puta prema dolje u jednoj epizodi komentira kako je napravio račun za internetsku stranicu *PayPal* ⁵⁴. Riječ je o tvrtci koja se bavi novčanim plaćanjem usluga preko Interneta. *PayPal* su osnovali Peter Thiel i Max Levchin 1998. godine te je jedna od najvećih organizacija koja se bavi internetskim plaćanjem. Podatci korisnika su zaštićeni i dostupni samo zaposlenicima *PayPala*. Unatoč poteškoćama s prijevarama i pranjem novca putem njegovih usluga, *PayPal* je i dalje najkorištenija usluga za plaćanje putem Interneta ⁵⁵.

Backgammon online

U epizodi serije Ubi me dosada glavni lik igra partiju tavle preko internetske stranice *www.backgammononline.com* ⁵⁶. Riječ je o internetskoj stranici na kojoj je moguće organizirati i igrati partije tavle protiv drugih igrača. Prije pristupa stranici

⁵¹ <http://money.howstuffworks.com/craigslist.htm>

⁵² Put prema dolje: ep. 312 - 3.45min

⁵³ <http://whatis.techtarget.com/definition/Wikipedia>

⁵⁴ Put prema dolje: ep. 212 - 19.57min

⁵⁵ <http://money.howstuffworks.com/paypal.htm>

⁵⁶ Ubi me dosada: ep. 101 - 7.19min

nužno je prijaviti se. Prijava je besplatna, a stranica omogućuje i igranje nekoliko partija protiv više protivnika odjednom ⁵⁷.

Soba za razgovor s računalnom sintezom govora

U američkom filmu *Mreža* Angela Bennett koristi sobu za razgovor (engl. *chat room*) s drugim informatičkim stručnjacima i hakerima. Prilikom pisanja teksta u sobi, računalo automatski provodi sintezu Angelinog teksta u govor (engl. text-to-speech, skraćeno *TTS*) ⁵⁸. Računalo provodi isti postupak i za tekst ostalih korisnika sobe. Film je snimljen 1995. godine. Iako bismo mogli pretpostaviti da je takva soba za razgovore proizvod dosjetljivog hakera ili programera, uobičajene sobe za razgovor u to doba nisu imale takvu mogućnost, a nemaju niti danas.

Laura Schindler u svojem članku godine opisuje projekt koji bi omogućio implementaciju programa za prepoznavanje govora i sintezu govora u sobe za razgovore kao pomagala za gluhe i slijepe ⁵⁹. Članak je iz 2005. godine. Sharma i Wasson su dizajnirali sobu za razgovore s istim mogućnostima 2012. godine, a iste godine je internetska stranica *SG World* najavila podršku za *TTS* u svojim sobama za razgovor ^{60 61}. Prema navedenim istraživanjima mogli bismo zaključiti da je *Mreža* prikazala element informatičke kulture koji je tek realno postao moguć minimalno 10 godina kasnije.

The Book World

U seriji *Obavještajci* jedan od likova pregledava internetsku stranicu *The Book World* ⁶². Ustvrdili smo kako navedena stranica ustvari ne postoji, iako postoji stvarna internetska stranica *Digital Book World* koja nema povezanosti s onom iz serije ⁶³. Najvjerojatniji razlog uporabi fiktivne stranice je zbog prije navedene politike *BBC-a* koji ne dopušta reklamiranje stvarnih proizvoda u svojim serijama, a i radi radnje.

⁵⁷ <http://backgammononline.com/>

⁵⁸ *Mreža*: 6.51min

⁵⁹ <http://www2.stetson.edu/~helaarag/Laura-proposal.pdf>

⁶⁰ http://www.ijcst.org/Volume3/Issue4/p17_3_4.pdf

⁶¹ <http://www.mynewsdesk.com/jp/pressreleases/sg-world-introduces-text-to-speech-an-innovative-virtual-world-featuring-tts-voice-for-global-english-chat-779340>

⁶² *Obavještajci*: ep. 307 - 34.09min

⁶³ <http://www.digitalbookworld.com/join/about/>

Pohranjenost stranica na računalu

U epizodi američke serije *Žica* par likova upotrebljavajući *MSN Search* pokušavaju otkriti svrhu određenih kemikalija. Prateći jednu poveznicu dođu do stranice koja objašnjava njihovu svrhu, no navedena stranica je otvorena u potpuno različitom prozoru od netom prije prikazanog *Internet Explorera* ⁶⁴. Također, uočljivo je kako URL adresa za novu stranicu ustvari pokazuje da se nalazi na tvrdom disku računala, točnije particije „C:“. Stoga možemo zaključiti da stranica ustvari ne postoji na Internetu, nego je napravljena za potrebe serije i pohranjena na tvrdom disku prije snimanja epizode.

3.6. Računalne mreže

U određenim slučajevima pojedinačna računala povezana su u skupove koji se zovu mrežama. U građi moguće je analizirati primjere koji se tiču stvarnih računalnih mreža. Većina proučene građe posvećuje se uporabi računalne i druge tehnologije zbog potrebe radnje. Prema analiziranim primjerima možemo vidjeti vjeran i tehnički ispravan prikaz i opis strukture, odnosno primjene današnjih računalnih mreža. Uz prisutnost općenitih činjenica, uočili smo i vrlo specifične opise te primjenu računalnih mreža zahvaljujući tehnološki orijentiranoj građi.

Network Address Translation

U Obavještajcima špijuni pokušavaju otkriti IP adresu osumnjičenika. Jedan od likova komentira kako navedenu IP adresu koriste stotine korisnika te ga je tako mnogo teže pratiti ⁶⁵. Postojanje jedne IP adrese na Internetu za više korisnika je svakodnevna situacija prilikom pristupanja Internetu u današnje doba. Ta pojava je omogućena pomoću Prijevoda mrežne adrese (engl. *Network Address Translation*, skraćeno *NAT*).

NAT je internetska norma koja služi u svrhu ograničavanja broja javnih IP adresa u organizacijama ili tvrtkama iz financijskih ili sigurnosnih razloga. Pomoću

⁶⁴ *Žica*: ep. 205 - 45.57min

⁶⁵ *Obavještajci*: ep. 307 - 13.35min

NAT-a se jedna IP adresa iz jedne mreže prevodi u drugu IP adresu koja postoji unutar druge mreže, odnosno prijevod iz „unutarnje“ mreže u „vanjsku“ mrežu. Tu zadaću najčešće izvršava mrežni uređaj poput *routera* ili vatrozida. Svako računalo unutar jedne mreže ima vlastitu IP adresu. Ako računalo šalje zahtjev za podacima koji se ne nalaze u mreži, nego na nekom drugom računalu na Internetu, zahtjev se proslijeđuje vatrozidu mreže koji vidi „unutarnju“ IP adresu računala te provodi zahtjev pomoću svoje „vanjske“ IP adrese. Pri povratku podataka s vanjskog računala, podatci se šalju na IP adresu vatrozida koji ih zatim proslijeđuje na IP adresu računala koje je podnijelo zahtjev. Iz perspektive vanjskog računala, zahtjev je zatražio vatrozid, a ne računalo unutar njegove mreže ⁶⁶.

NAT je vrlo koristan, budući da omogućuje manji broj nužnih javnih IP adresa za pristup podacima preko kojih se mogu potvrditi svi zahtjevi i podatci koji prolaze kroz vatrozid. Također je bitno naglasiti kako većina današnjih vatrozida može pratiti stanje uspostavljene veze između računala i Interneta. Nakon što se veza završi, vatrozid briše sve podatke o vezi ⁶⁷. Stoga možemo zaključiti kako je scena unutar epizode serije sasvim realna situacija ako je locirana IP adresa javna adresa *routera* ili vatrozida neke mreže.

Apsolutna URL adresa

U filmu *Mreža* Angela pregledava internetsku stranicu s URL adresom „*http://link_jas.com*“ ⁶⁸. Iako navedena stranica – barem danas – ne postoji, struktura URL adrese je ispravna. Riječ je o apsolutnoj URL adresi, budući da osim domene „*link_jas.com*“ sadrži i protokol koji je u ovom slučaju „*http://*“ ⁶⁹. Da stranica postoji, mogli bismo joj pristupiti ovakvom adresom.

Podmreža

Također u *Mreži*, jedan od likova na početku filma objašnjava kako je pristupio dijelu tvrtkine mreže kojoj ne bi smio imati pristup. Komentira da je taj dio mreže na

⁶⁶ <http://searchenterprisewan.techtarget.com/definition/Network-Address-Translation>

⁶⁷ <http://whatismyipaddress.com/nat>

⁶⁸ *Mreža*: 10.22min

⁶⁹ <https://kb.iu.edu/d/abwp>

drukčijoj podmreži od njegove (engl. *subnet*) ⁷⁰. Podmreža je jasno odijeljeni dio mreže neke ustanove. Razlog upotrebljavanja podmreža je što pomoću njih mreža ustanove može biti spojena na Internet pomoću samo jedne mrežne adrese koju koriste sve podmreže. Iako bi bilo moguće da svaka podmreža posjeduje vlastitu mrežnu adresu za pristup Internetu, time bi se trošilo više raspoloživih mrežnih brojeva koji se na Internetu mogu pripisati nekoj mreži nego je nužno ⁷¹. Bez podmreža bi se i usmjeravanje (engl. *routing*) podmreža trebalo obavljati izvan ustanove koja ih upotrebljava, stoga možemo zaključiti kako je prednost podmreža da omogućuju i dodatnu razinu sigurnosti svoje mreže.

Proxy serveri

U filmu *Kick-Ass 2* glavni likovi pokušavaju otkriti koju IP adresu upotrebljava glavni negativac, no njihov informatički stručnjak objašnjava kako je njegova IP adresa „maskirana“ ⁷². Kad se računalo spaja na Internet, pripisuje mu se javna IP adresa koja posjećivanjem internetskih stranica ostaje u zapisima servera na Internetu. Pomoću tih zapisa moguće je vidjeti čemu je računalo pristupalo te ga preko IP adrese pratiti do ishodišne točke. Ako korisnik ne želi da ga se naknadno može pratiti, potrebno je sakriti, tj. „maskirati“ IP adresu. Najuočividniji način skrivanja vlastite IP adrese je uporabom *proxy* (hrv. zamjenski) servera.

Proxy server se prema riječima Bradleyja Mitchella ponaša kao „posrednik“ između računala i ostatka Interneta ⁷³. Postoji nekoliko vrsta *proxy* servera: transparentni, anonimni, distorzijski i elitni ⁷⁴. Transparentni *proxy* serveri ustvari prosljeđuju IP adresu korisnika, stoga ne pružaju veliku razinu anonimnosti. Anonimni serveri ne prosljeđuju korisnikovu IP adresu, ali se na Internetu predstavljaju kao zamjenski server, dok npr. distorzijski server (engl. *distorting*) daje netočnu IP adresu korisnika ⁷⁵. Najsigurniji *proxy* serveri su elitni serveri (engl. *high anonymity*) koji ne prosljeđuju IP adresu korisnika i ne predstavljaju se kao zamjenski serveri. Anonimni serveri mogu biti besplatni, ali takvi serveri najčešće nisu najpouzdaniji te imaju

⁷⁰ Mreža: 13.05min

⁷¹ <http://searchnetworking.techtarget.com/definition/subnet>

⁷² *Kick-Ass 2*: 1.05.13h

⁷³ <http://compnetworking.about.com/od/workingwithipaddresses/f/hideipaddress.htm>

⁷⁴ <http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-08-309.pdf>

⁷⁵ <http://computer.howstuffworks.com/internet/basics/hide-ip-address.htm>

poteškoće s brzinom i ograničenja širine pojasa. Anonimni zamjenski serveri uz naplatu nude bolju uslugu i sigurnost prilikom korištenja. Upotreba besplatnih servera ovisi o potrebama korisnika, ali se najčešće preporuča kao privremeno rješenje.

4. PROGRAMI

U popularnoj kulturi često možemo vidjeti primjere različitih programa koji su prikazani zbog potrebe radnje ili su upotrijebljeni kao pozadinski detalj. Dok u nekim slučajevima možemo vidjeti primjenu programa u njihovu stvarnu svrhu, ponekad služe kao zamjena za druge, bilo stvarne, bilo izmišljene programe. Proučena građa se sastojala od filmova i serija različitih žanrova i tematika te različite razine tehnološke preciznosti. Navedeni primjeri stoga variraju u vjernosti i preciznosti prikaza, ali možemo pretpostaviti kako je omjer podjednak te uglavnom ovisi o vrsti građe i njenoj svrsi.

4.1. Sigurnosne snimke

U raznim kriminalističkim i sličnim serijama možemo vidjeti sigurnosne snimke koje služe za napredak radnje. Njihova vjerodostojnost varira ovisno o izvoru te je uočena mogućnost temelja u stvarnoj tehnologiji i primjeni, ali se najčešće pribjegava različitim – uočljivim - alternativama.

Zapisi nadzornih kamera

U epizodi humoristične serije *Brooklyn Nine-Nine* detektiv Peralta svom nadređenom pokazuje video zapis sa sigurnosne kamere iz policijske postaje ⁷⁶. U epizodi *Broadchurche* istražitelji pregledavaju snimku nadzorne kamere kako bi

⁷⁶ *Broadchurch*: ep. 101 - 43.53min

utvrdili kretnje žrtve prije smrti ⁷⁷. U oba slučaja je rezolucija snimke relativno dobre kvalitete, dok prijenos varira u kvaliteti. Dok je u *Brooklyn Nine-Nine* zapis mnogo bolje kvalitete, u *Broadchurchu* je zapis vidljivo isprekidan. Razlog isprekidanosti zapisa bi mogao biti pokušaj da se uštedi na pohrani video zapisa.

Budući da se za pohranu snimaka upotrebljavaju tvrdi diskovi ograničenog prostora, često se upotrebljavaju različite tehnike kako bi zapis zauzimao što manje prostora ⁷⁸. U slučaju *Broadchurcha* možemo vidjeti da je broj sličica po sekundi (engl. *frame per second*, skraćeno FPS) znatno manji od standardnih 24, dok je u *Brooklyn*u broj 24 ili više. Što je manji broj sličica u sekundi, zapis zauzima manje prostora ⁷⁹. Broj sličica može varirati ovisno o potrebi. Budući da video zapis iz *Brooklyn*a snima skladište s dokazima, možemo pretpostaviti kako zbog sigurnosti zapis mora biti bolje kvalitete iz sigurnosnih razloga. U *Broadchurchu* je zapis najvjerojatnije isprekidan zato što je scena snimanja po noći kada ima manje aktivnosti na ulicama te nema potrebe za većim brojem sličica.

Sigurnosne snimke i Windows Media Player

U epizodi američke serije *Sinovi Anarhije*, antagonisti epizode proučavaju sigurnosnu snimku na kojoj se vidi jedan od glavnih likova serije ⁸⁰. Jasno se vidi da je snimka ustvari video zapis koji je otvoren u programu za reprodukciju *Windows Media Player* koji je instaliran sa svakom verzijom operativnog sustava *Windows* ⁸¹. Program također podržava reprodukciju zvučnih datoteka te snimanje sadržaja na prijenosne medije. Još jedan uočljivi detalj ukazuje na to da zapis nije stvarna sigurnosna snimka. U jednom trenutku je zapis zaustavljen, no klizač koji pokazuje trajanje snimke i dalje se vidljivo miče, odajući da je videozapis unaprijed snimljen za potrebe serije, a ne stvarna snimka.

U epizodi britanske znanstveno-fantastične serije *Jekyll*, glavni negativac čeka dolazak glavnog lika. U jednom trenutku ga uoči na sigurnosnoj snimci koju prati na

⁷⁷ *Brooklyn Nine-Nine*: ep. 110 - 8.23min

⁷⁸ <http://www.cbc.ca/news/canada/hamilton/news/why-is-security-camera-video-still-so-terrible-1.2542359>

⁷⁹ <http://www.securitycameraking.com/securityinfo/what-is-fps-frames-per-second/>

⁸⁰ *Sinovi anarhije*: ep. 205 - 13.49min

⁸¹ <http://www.winxdvd.com/resource/windows-media-player.htm>

svojem prijenosnom računalu ⁸². Međutim, i u ovoj seriji je jasno vidljivo da lik gleda reprodukciju s *Windows Media Playera* koji reproducira unaprijed snimljeni video zapis, a ne stvarnu sigurnosnu snimku. Možemo zaključiti da se problem u oba slučaja mogao jednostavno riješiti reproduciranjem video zapisa u punom prikazu (engl. *fullscreen*), funkcijom koju podržava svaki program za reprodukciju, tako i *WMP*.

4.2. Računalne igre

S obzirom na njihovu rasprostranjenost, računalne igre imaju sve veću zastupljenost u različitim medijima. Mogu biti fizički prisutne u primjerima ili samo spomenute. Većina proučenog sadržaja nastala je u prvom desetljeću 20.-tog stoljeća kad su računalne igre postale opća spoznaja. Unatoč tome postoji nekoliko starijih primjera koji imaju neujednačeni tehnološki prikaz unutar istog izvora. Prema analiziranoj građi se vidi upoznatost s današnjom kulturom računalnih igara, uključujući i fiktivne primjere koji se temelje na trenutnim trendovima u igrama.

Wolfenstein 3D

U jednom od prvih prizora u *Mreži Angela* testira računalnu igru *Wolfenstein 3D* ⁸³. Riječ je o jednoj od najpoznatijih računalnih igara iz žanra „pucačina iz prvog lica“ (engl. *First Person Shooter*, skraćeno *FPS*). Izvorno je izdana za operativni sustav *MS-DOS* 1992. godine, a naknadno su napravljene verzije i za druge operativne sustave ⁸⁴. Angela Bennett igru testira na *Appleovom* računalu koje upotrebljava operativni sustav *Mac OS*, a verzija *Wolfensteina 3D* za taj sustav izdana je 1994. godine, tj. godinu dana prije pojavljivanja filma u kinima ⁸⁵.

Angela u filmu ima pristup izvornom kodu igre kako bi je mogla ispravno testirati ⁸⁶. Izvorni kod je niz programskih naredbi koje programer piše u predodređenom alatu ili programu za uređivanje teksta te pohranjuje u datoteku. Sve

⁸² Jekyll: ep. 106 - 28.50min

⁸³ Mreža: 3.34min

⁸⁴ http://wolfenstein.wikia.com/wiki/Wolfenstein_3D

⁸⁵ <http://theodor.lauppert.ws/games/wolfmac.htm>

⁸⁶ Mreža: 4.10min

naredbe izvornog koda imaju specifičnu namjenu u programu prilikom njegovog pokretanja. Izvorni kod se zatim pomoću jezičnog prevoditelja (engl. *compiler*) prevodi u objektni kod koji procesor može čitati. Dok je izvorni kod čitljiv, objektni kod programer ne može čitati niti izmjenjivati. Korisnici većine programa nemaju pristup izvornom kodu kako ga ne bi mogli mijenjati bez dopuštenja programera ⁸⁷. Neki programi se ipak izdaju s izvornim kodom, a za neke se kod naknadno izdaje. Izvorni kod *Wolfensteina 3D* izdan je 21. srpnja 1995. godine, a film Mreža u SAD-u je izdan 28. srpnja iste godine ⁸⁸.

U ovom slučaju možemo uočiti nekoliko problema s filmom. Iako je film izdan nakon što je izvorni kod postao javan, zasigurno nije pušten u javnost dok je film bio u fazi produkcije i snimanja. Također je bitno uočiti da je igra u filmu opisana kao novi proizvod za *Mac OS*, unatoč tome što je verzija za isti sustav izdana godinu dana ranije. Angela Bennett nije dakle imala nikakvog razloga pregledavati izvorni kod računalne igre koja je već bila izdan i testiran proizvod na sustavu koji ona upotrebljava.

Left 4 Dead, Resident Evil 4 i Call of Duty – World at War

U epizodi Puta prema dolje dva lika – *Badger i Skinny Pete* – raspravljaju o računalnim igrama u kojima se igrač bori protiv zombija. Za vrijeme scene navode tri računalne igre: *Left 4 Dead, Resident Evil 4 i Call of Duty – World at War* ⁸⁹. Sve tri navedene igre su stvarne igre u kojima su prisutni zombiji kao negativci.

Left 4 Dead je FPS od proizvođača *Valve Corporation*. Izdan je 18. studenog 2008. godine za osobna računala kao igra koja se igra preko Interneta sa sveukupno 4 igrača ⁹⁰. *Resident Evil 4* je akcijska igra iz trećeg lica koju je proizveo japanski *Capcom Production Studio 4*, podružnica izdavača *Capcom* te je izdana 11. siječnja 2005. godine za igraču konzolu *Nintendo Gamecube*, a kasnije za *Sony Playstation 2* i osobna računala ⁹¹. *Call of Duty – World at War* također je FPS smješten u doba Drugoga svjetskog rata i izdan je 2008. godine. Igra sadrži poseban način igranja u

⁸⁷ <http://searchsoa.techtarget.com/definition/source-code>

⁸⁸ http://wolfenstein.wikia.com/wiki/Wolfenstein_3D_source_code

⁸⁹ Put prema dolje: ep. 402 - 9.34min

⁹⁰ http://left4dead.wikia.com/wiki/Left_4_Dead

⁹¹ http://residentevil.wikia.com/Resident_Evil_4

kojem se igrač sukobljava s nacističkim zombijima ⁹². Iako je epizoda koja opisuje navedene igre emitirana 7. kolovoza 2011. godine, opisane igre i dalje su poznate te popularne.

Igre kretnjom

U američkom znanstveno-fantastičnoj drami Ona Theodore Twombly igra računalnu igru koristeći se kretnjama svojih nogu i ruku kako bi napredovao ⁹³. Riječ je o igri kretnjom iako je riječ o vrsti igre koja je naprednija nego današnje igre. Prva igrača konzola koja je omogućila igranje koristeći kretanje korisnikovog tijela bio je *Nintendo Wii* 2006. godine. Kasnije su i druge igrače konzole uvele ovakvu podršku za igranje poput *Kinecta* za *Microsoftov Xbox 360* te *Move* za *Sonyjev Playstation 3*. Razlika u implementaciji tehnologije za sve tri konzole svodila se na način koji se upravljalo njima.

Dok su *Nintendo Wii* i *Playstation Move* ovisili o uporabi ručnih kontrolera koji su sličili daljinskim upravljačima, *Kinect* je omogućavao uporabu bez kontrolera. U svaku konzolu je ugrađena kamera koja prati kretanje kontrolera kod *Wiija* i *Movea*, odnosno samog korisnika kod *Kinecta*. Kinectova tzv. „dubinska kamera“ zapisuje kretanje korisnika u trodimenzionalnom prostoru i prati sve njegove pokrete prilikom igranja ⁹⁴. Način uporabe kretanje za igranje u filmu znatno je napredije nego što današnja tehnologija omogućuje, no u skorijoj budućnosti bi i takva implementacija bila moguća, osobito s poboljšanjem senzora kretanje u konzolama.

4.3. Prepoznavanje lica

Programi za prepoznavanje lica su često prikazani u različitim kriminalističkim serijama zbog razvoja radnje. U ovom smo slučaju posvetili se jednom specifičnom primjeru i analizirali ga kako bismo utvrdili na koji način je prikazana primjena i koliko je vjerodostojna stvarnoj tehnologiji. Možemo uočiti kako se primjer temelji na stvarnoj tehnologiji, ali zbog nekoliko bitnih razloga ne funkcionira na način prikazan

⁹² http://callofduty.wikia.com/wiki/Call_of_Duty:_World_at_War

⁹³ Ona: 5.43min

⁹⁴ <http://whatis.techtarget.com/definition/motion-gaming-motion-controlled-gaming>

u seriji. Iako neke greške nisu ozbiljne, i dalje iskrivljuju percepciju mogućnosti programa.

Biometrijska analiza

U epizodi Obavještajaca možemo vidjeti uporabu programa za identifikaciju osobe ⁹⁵. Prepoznavanje lica je vrsta biometrijske analize i usporedbe digitalnih slika kako bi mogli prepoznati određenog pojedinca. Proces prepoznavanja lica pomoću računala započeo je 1960-ih godina.

Prije negoli je moguće osobu prepoznati, nužno je imati pohranjene slike njenog lica. Svako lice je jedinstveno i posjeduje specifične karakteristike koje je kasnije moguće prepoznati pomoću programa. Programi za prepoznavanje lica definiraju te karakteristike kao čvorišne točke (engl. *nodal points*), a pretpostavlja se da svaka osoba posjeduje oko 80 specifičnih točaka lica. Neke od točaka koje programi mjere su razmak između očiju, širina nosa, dubina očnih duplji, oblik jagodica te duljina čeljusti. Tako pohranjena slika lica zove se „otiskom lica“ (engl. *faceprint*) ⁹⁶.

Kako bi se lice usporedilo s bazom podataka, slika se iz različitih kutova i s različitim izrazima lica, a kako bi se spriječilo korištenje fotografija ili maska nove mjere sigurnosti uključuju potrebu da se korisnik nasmije, zatrepće ili kimne glavom. No treba naglasiti kako je ovakav postupak moguć samo u kontroliranim uvjetima. Većina slika koje treba usporediti s bazom podataka nije napravljena u idealnim uvjetima. Problemi često nastaju zato što bilo kakve izmjene u osvjetljenju ili orijentiranosti te izrazu lica mogu dovesti do slabijih konačnih rezultata. Znatniju prednost u prepoznavanju lica stoga ima trodimenzionalno prepoznavanje lica koje upotrebljava 3D senzore kako bi zapisalo oblik lica ⁹⁷. Prednosti takvog prepoznavanja su u tome što je osobu moguće prepoznati i pod slabijim svjetlom te pod kutevima gledanja od čak 90 stupnjeva, odnosno iz profila ⁹⁸.

⁹⁵ Obavještajci: ep. 203 - 7.18min

⁹⁶ <http://whatis.techtarget.com/definition/facial-recognition>

⁹⁷ <http://findbiometrics.com/solutions/facial-recognition/>

⁹⁸ <http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm>

U navedenoj sceni glavni likovi pokušavaju prepoznati lice čovjeka pomoću standardnog biometrijskog prepoznavanja. Vidljivo je da se za potrebe prepoznavanja uspoređuju različiti dijelovi lica. Prema prikazanim slikama možemo pretpostaviti da se uspoređuje razmak između očiju, oblik jagodica, očne duplje i oblik usta. Iako je osvijetljenost lica dobra, osoba ne gleda izravno u kameru, te je njeno lice snimljeno iz poluprofila i pognuto je. Stoga je ovakvu sliku uobičajenom tehnikom prepoznavanja lica teže prepoznati i najvjerojatnije program ne bi tako brzo prepoznao osobu na slici. Također, slika iz rezultata je također snimljena iz poluprofila i iz niže pozicije te bi rezultat pretrage mnogo vjerojatnije bila slika u kojoj osoba izravno gleda u kameru i u ravnini je s njome. Tehnologija dakle postoji, ali najvjerojatnije ne bi funkcionirala na način prikazan u seriji.

4.4. Programi za obradu slike

Programi za obradu slike često se pojavljuju ako treba izmijeniti sadržaj ili istražiti je li slika u pitanju obrađena. Pristup takvim programima ovisi o vrsti serije, ali i o potrebi radnje. Prema analiziranim primjerima prikaz programa u većini slučajeva nije realan. Mogućnosti obrade slike često su pretjerane zbog potrebe radnje, a ponekad u potpunosti graniče s današnjom tehnologijom. Moguće je zamijetiti kako postoji nekoliko slučajevima u kojima se naglašavaju ograničenja kod obrade, iako potječu iz građe koja istovremeno prikazuje potpuno suprotne rezultate.

Photoshop

Većina korisnika računala već se susrela ili je barem čula za *Adobe Photoshop*. Riječ je o jednom od najpopularnijih programa za digitalnu obradu i uređivanje slika. U epizodi *Sinova Anarhije* jedan od glavnih likova Juice Ortiz spominje uporabu *Photoshopa* za obradu jedne slike⁹⁹. Iako program nije prikazan, sama rečenica referira na njega kao specifični program, a ne općenito na bilo koji program za digitalnu obradu slike.

⁹⁹ Sinovi anarhije: ep. 505 - 24.05min

U Obavještajcima stručnjak za računala Malcolm spominje da je na slici pregledao područje oko ušiju i vrata jedne osobe, napominjući kako su to najčešća mjesta gdje se mogu uočiti mane prilikom digitalne obrade slike u *Photoshopu* ¹⁰⁰. Prilikom digitalne obrade slike – osobito ako se sadržaj manipulira i izmjenjuje – može doći do neujednačenosti piksela na područjima lica koja se obrađuju. Takve neujednačenosti se nazivaju „ožiljcima“ (engl. *scarring*) ¹⁰¹. Dodavanjem drukčijeg sadržaja rezolucija sadržaja se često ne podudara s izvornom rezolucijom slike. U slučaju epizode ako bi netko zamijenio lice osobe na slici, rezolucija se najvjerojatnije ne bi podudarala s rezolucijom ostatka slike, a područja na kojima bi se to uočilo bi najvjerojatnije bile uši i vrat kao što je navedeno.

4.4.1. Uvećavanje i izoštravanje slike

Kod programa za obradu slike također dolazimo do primjera u kojima je moguće primjetiti različite procese uvećavanja i izoštravanja slika. Iako postoji nekoliko realnih primjera upotrebe tehnologije, mnogo su češći primjeri u kojima su programi upotrijebljeni u situacijama u kojima ne bi bilo moguće dobiti kvalitetne rezultate. Kako bismo razlikovali primjenu programa za obradu zbog volumena analizirane građe, podijelit ćemo je na temelju mogućnosti programa.

Realna primjena

U epizodi Obavještajaca možemo vidjeti izoštravanje slike putem računala, primjer koji se često pojavljuje u serijama s tehnološkom tematikom ¹⁰². Bitno je napomenuti kako mogućnosti obrade ovise o alatima koji se upotrebljavaju, tako ovise i o vrsti slike koja se obrađuje.

Mogućnost izmjene slike ovisi o količini podataka koje ona sadrži. Goodnight uspoređuje pohranu slika navodeći analogne i digitalne fotoaparate koji pohranjuju slike različitim metodama, ali se kvaliteta pohranjenog sadržaja temelji na istom

¹⁰⁰ Obavještajci: ep. 409 - 17.58min

¹⁰¹ McClelland, D.: str. 132.

¹⁰² Obavještajci: ep. 405 - 33.30min

principu – količini raspoloživih podataka u trenutku slikanja ¹⁰³. Svaka slika ima fiksnu količinu podataka koju nije moguće naknadno povećati. Sve ovisi o kvaliteti i rezoluciji slike koju pokušavamo obraditi.

U spomenutoj epizodi Obavještajaca ne vidimo konačni rezultat izoštravanja zamućene slike – tehničar Malcolm komentira kako će proces potrajati i nije siguran u ishod – dok u nekim serijama vidimo slične situacije s različitim ishodom. Detektiv Luther u epizodi istoimene britanske serije proučava snimku s nadzorne kamere kao bi otkrili identitet počinitelja. Na pitanje može li se snimka poboljšati, kolega mu odgovara kako ishod neće biti pozitivan, budući da je rezolucija snimke vrlo niska ¹⁰⁴.

Fiktivna primjena

Međutim, u nekim slučajevima vidimo primjere izoštravanja slike, čak i u slučajevima gdje to ne bi smjelo biti moguće. U epizodi Obavještajaca je prikazan slučaj otkrivanja kad je slika napravljena na temelju novina na kojima je naveden datum. Kako bi jasno mogli pročitati datum, tehničari uvećavaju dio slike koji sadrži novine što dovodi do mnogo jasnije slike novina ¹⁰⁵. Možemo pretpostaviti da je u neprikazanoj sceni taj dio slike izoštren pomoću različitih alata, iako je vidljivo da je izvorna slika niže rezolucije te rezultat ne bi bio bolje kvalitete od izvorne slike. U epizodi Luthera glavni lik može izoštriti sliku registracijske tablice vozila s nadzornih kamera snimljenog iz veće udaljenosti ¹⁰⁶. Rezultat je vrlo oštri prikaz tablice, nešto što nije moguće, budući da je upotrijebljen uvećani dio slike koja je izvorno vrlo niske rezolucije. Zanimljiva je činjenica kako su oba primjera iz serija u kojima je također bilo moguće vidjeti primjere negativnog rezultata izoštravanja sadržaja. U Obavještajcima prvo vidimo primjer realnije obrade, a zatim nemoguće obrade, dok u Lutheru imamo suprotni slučaj – prvo je prikazana nerealna scena, zatim realna. Možemo zaključiti da je ova nedosljednost posljedica odluke scenarista da se više posvete potrebama radnje, negoli vjernijem prikazu stvarnosti.

Ponovno dolazimo do zaključka kako nije moguće izoštriti sliku ako nema dovoljno izvornih podataka, iako postoje algoritmi koji omogućuju uklanjanje loših

¹⁰³ <http://www.howtogeek.com/howto/43078/stop-believing-tvs-lies-the-real-truth-about-enhancing-images/>

¹⁰⁴ Luther: ep. 203 - 12.09min

¹⁰⁵ Obavještajci: ep. 409 - 17.34min

¹⁰⁶ Luther: ep. 104 - 17.40min

podataka kako bismo mogli doći do boljeg konačnog rezultata ¹⁰⁷. Čak i uz takve alate, i dalje nije moguće postići neke rezultate koje smo mogli vidjeti u navedenim serijama. Iako postoje mnogo neuvjerljiviji primjeri, u ovom smo se slučaju pridržali primjera koji nisu toliko nevjerojatni.

Među primjerima koji dosežu granice današnje tehnologije možemo navesti epizodu američke serije *CSI: NY*. U navedenoj epizodi glavni likovi uspijevaju sa sigurnosne snimke žrtve uvećati i izoštriti sliku osumnjičenika odraženu u oku žrtve ¹⁰⁸. Mada je nužno napomenuti kako je pomoću odgovarajuće opreme moguće vidjeti odraze predmeta i ljudi u očima ljudi sa slika, potrebna je vrlo kvalitetna i precizna oprema za dobivanje slika dovoljno visoke rezolucije za obradu ¹⁰⁹. U epizodi je odraz dobiven sa snimke koja je vrlo niske rezolucije te žrtva nije snimljena pod ispravnim kutom kako bi se mogao vidjeti točni odraz počinitelja. Unatoč postojanju takve tehnologije, konačni rezultat ne bi bio ni približan dobivenom.

4.5. Programi za prisluškivanje

Programi za prisluškivanje česta su pojava u žanrovima koji se fokusiraju na uporabu tehnologije. Unatoč postojanju takvih programa, u analiziranoj građi nije primijećena njihova prisutnost. Navedeni primjeri prikazuju programe koji inače imaju drukčiju funkciju od prisluškivanja. Može se pretpostaviti kako su takvi programi upotrijebljeni zbog vrlo kratke prisutnosti unutar radnje, dok većina gledatelja nije upoznata s njihovim izgledom te ih ne bi mogla razlikovati. Primjeri su podijeljeni prema vrsti programa koja je prikazana te je pojašnjena njihova stvarna primjena.

Pro Tools

U Sinovima anarhije možemo vidjeti scenu prisluškivanja telefonske linije u kojoj je moguće vidjeti program za prisluškivanje ¹¹⁰. Iako je program prikazan kao program za prisluškivanje, ustvari je riječ o programu *Pro Tools* koji se upotrebljava za profesionalno snimanje i obradu zvuka u glazbenoj industriji. Na radnoj površini

¹⁰⁷ <http://www.asmag.com/showpost/12849.aspx>

¹⁰⁸ *CSI: NY*: ep. 110 – 31.20min

¹⁰⁹ http://www1.cs.columbia.edu/CAVE/projects/world_eye/

¹¹⁰ Sinovi anarhije: ep. 210 - 8.49min

programa također je vidljiv natpis „*Digidesign*“ što je ime tvrtke koja je napravila *Pro Tools*, a kasnije je postala dijelom tvrtke *Avid* ¹¹¹.

Iako je *Pro Tools* program za obradu, za njegovo potpuno funkcioniranje nužno je imati i odvojeno audio sučelje za povezivanje s analognim uređajima prilikom obrade. U sceni je moguće vidjeti da je na prijenosno računalo spojeno audio sučelje marke *Mbox* koje je među manjim varijantama sučelja za povezivanje samo nekoliko ulaznih jedinica ¹¹². Prema ovome možemo zaključiti kako ovakva vrsta opreme za obradu zvuka ne bi bila korištena za potrebe prisluškivanja telefonskih linija.

Program za transkripciju

U epizodi *Žice* možemo vidjeti drugi primjer programa za prisluškivanje koji se jasno može vidjeti u sceni epizode ¹¹³. No – kao i kod *Sinova anarhije* – i ovdje je riječ o potpuno drukčijem programu od onih koji bi se upotrebljavali za prisluškivanje. Prema izgledu i dizajnu programa očito je da je riječ o programu za prijepis, odnosno transkripciju snimljenog govora. Programi za transkripciju upotrebljavaju se u situacijama kada je potrebno snimljeni govor prenijeti u pisani oblik za potrebe čitanja. Takvi programi primarno se upotrebljavaju ako se proces transkripcije provodi na računalu. Osoba koja prepisuje mora preslušati zvučni zapis i zaustavljati ga kako bi zapisala što je rečeno. Na taj se način tekst kasnije može povezati s dijelovima zvučnog zapisa. Neki programi također prikazuju valni oblik zapisa prilikom reprodukcije ¹¹⁴.

Argumenti da je u epizodi upotrijebljen program za transkripciju, a ne za prisluškivanje je u činjenici da je vidljiv natpis da je program namijenjen za prepisivanje. Također se mogu vidjeti rezultati prijepisa govora, no prikazani dio teksta ne podudara se sa zvučnim zapisom koji čujemo u sceni, a budući da je sadržaj već bio preslušan, očekuje se da je tekst u potpunosti prepisan radi istrage. Stoga možemo zaključiti kako je i u ovom slučaju upotrijebljen uobičajeni komercijalni

¹¹¹ <http://entertainment.howstuffworks.com/pro-tools-software-hardware.htm>

¹¹² <http://www.avid.com/US/products/mbox>

¹¹³ *Žica*: ep. 209 - 5.44min

¹¹⁴ <http://sophia.smith.edu/~jdrisko/transcription.htm>

produkt s prikazom valnog oblika zvučnog zapisa, a s kojim većina gledatelja najvjerojatnije ne bi bila upoznata.

5. RAČUNALNA SIGURNOST

Računalna sigurnost je vrlo česta pojava u građi, osobito u trilerima i serijama koje se bave tehnologijom i računalnim sustavima. Preciznost u prikazu ovisi o nekoliko faktora. Nužno je utvrditi je li prikaz tehnologije glavni fokus radnje ili je prikaz sekundaran glavnoj radnji. U proučenoj građi možemo uočiti prisutnost stvarnih primjera, ali i fiktivnih. Točnost u opisima ovisi primarno o vrsti proučenog medija. Dok je u većini građe s fokusom na računalnu tehnologiju većina prikaza i opisa tehnički precizna i ispravna, u nekim slučajevima je većina primjera netočna u prikazu ili opisu, unatoč činjenici što su glavni fokus radnje. Razlog takvom odstupanju možemo pripisati prisutnosti, odnosno odsutnosti tehničkih savjetnika što je utjecalo na vjerodostojnost sadržaja prilikom analize. Uočljiva je i prisutnost tehničkih savjeta kad je informatika u sekundarnoj funkciji precizno prikazana. U nekim primjerima se odstupalo od točnosti više zbog dramatičnog doživljaja, nego prikaza stvarnosti. Kod sekundarne funkcije preciznim prikazom dolazi do veće posvećenosti informatici i primarno je ovisna o prisutnosti tehničkih savjetnika.

5.1. Lozinke

Lozinke su vrlo česte u proučenoj građi, a pristup im varira ovisno o potrebi radnje ili vjernosti njihovoj primjeni. Prema analiziranim primjerima možemo zaključiti kako su lozinke precizno prikazane i sukladne stvarnoj primjeni. Iako postoje odstupanja, većina je više iz umjetničkih razloga nego praktičnih.

Vidljivost lozinke

Prilikom unosa lozinke ne bismo smjeli vidjeti njen sadržaj iz sigurnosnih razloga. Stoga se u današnjim sustavima za očuvanje sigurnosti podataka lozinke maskiraju pomoću posebnih znakova kako ih neovlašteni pojedinci ne bi mogli vidjeti ispisane. Maskiranje se provodi pomoću znakova za nabranje kao što su asterisk ili crna točka. U mnogim filmovima i televizijskim serijama današnjice prikaz unosa lozinke sukladan je stvarnom načinu unosa, tj. lozinka je skrivena posebnim znakovima, što je moguće vidjeti prema proučenoj građi. U američkim filmovima *Hakeri* i *Mreža* prilikom unosa lozinke ne vidimo njen sadržaj ^{115 116 117}. Isti slučaj je i sa britanskim serijama *Doktor Who* i *Luther* ^{118 119}.

Iako je tendencija skrivenih lozinki česta, postoje i iznimke. Na početku filma *Hakeri* možemo vidjeti kako jedan od glavnih likova unosi lozinku za pristup strogo čuvanom sustavu ¹²⁰. Sličnu situaciju možemo vidjeti i u filmu *Mreža* ¹²¹. Zanimljiva je činjenica kako su oba primjera iz filmova koji su također imali i realne primjere maskiranih lozinki. Kod *Hakera* možemo argumentirati da je lozinka prikazana iz dramatičnih razloga – budući da je u pitanju riječ „Bog“ (engl. *god*) – no u *Mreži* lozinka ne sadrži nikakvo posebno značenje koje bi gledatelj trebao uočiti. Dapače, u *Hakerima* je lozinka prikazana na velikom ekranu te je mogu pročitati svi promatrači u blizini ekrana, što dodatno upućuje na neuvjerljivost scene i dramatičnost. Možemo napomenuti kako je u *Mreži* prikazan postupak maskiranja lozinke, ali tek nakon što je u potpunosti unesena i vidljiva na ekranu te možemo zaključiti da je razlog tome isti kao i za *Hakere*.

Najčešće korištene lozinke

U *Hakerima* likovi nabrajaju najčešće korištene lozinke. Među navedenim lozinkama su „ljubav“, „tajna“, „seks“ i „Bog“ (engl. *love, secret, sex, God*) ¹²². Prema popisima najčešćih lozinaka koje korisnici upotrebljavaju možemo vidjeti i dalje čestu

¹¹⁵ *Hakeri*: 19.01min

¹¹⁶ *Hakeri*: 1.14.23h

¹¹⁷ *Mreža*: 58.15min

¹¹⁸ *Doktor Who*: ep. 106 - 19.23min

¹¹⁹ *Luther*: ep. 204 - 38.40min

¹²⁰ *Hakeri*: 26.04min

¹²¹ *Mreža*: 55.43min

¹²² *Hakeri*: 24.44min

uporabu lozinke „god“, „love“, „sex“ i „secret“^{123 124}. Istraživanja pokazuju kako korisnici često upotrebljavaju jednostavne nizove znakova, najčešće imenice poput navedenih primjera¹²⁵. Iako neki noviji popisi najčešćih lozinaka ne sadrže navedene primjere, jednostavne riječi i dalje se upotrebljavaju^{126 127}.

Lozinka za tvorničke postavke

U epizodi Obavještajaca saznajemo kako su usmjerivači (engl. *router*) jedne tvrtke postavljeni s lozinkom od tvorničkih postavki – lozinkom „password“¹²⁸. Spomenuta lozinka je česta kad su *routeri* namješteni na tvorničke postavke. Među proizvođačima koji imaju modele s navedenom lozinkom su *Samsung* s modelom AHT-E300 i *Apple* s modelom bazne stanice *Airport Base Station (Dual Ethernet) Rev. 2*¹²⁹.

5.2. Kriptografska zaštita

Kriptografska zaštita je jedan od primjera računalne sigurnosti koje možemo uočiti u građi, a često se pojavljuje ako je tematika industrijska špijunaža ili krađa. Prema analiziranom sadržaju većina primjera zaštite je stvarna ili se temelji na stvarnoj tehnologiji. U nekim slučajevima možemo međutim uočiti neispravnu primjenu zaštite u kontekstu radnje, iako je precizno opisana. Razlog može biti u nepostojanju tehničkih savjetnika koji bi mogli osigurati preciznost što dovodi do nelogičnosti u sadržaju.

¹²³ <http://mashable.com/2012/06/08/linkedin-stolen-passwords-list/>

¹²⁴ <http://www.computerhope.com/issues/ch000300.htm>

¹²⁵ Kissell, J. Are Your Passwords Safe

¹²⁶ <http://www.dailymail.co.uk/sciencetech/article-2223197/Revealed-The-common-passwords-used-online-year-password-STILL-tops-list.html>

¹²⁷ <http://www.cbsnews.com/news/the-25-most-common-passwords-of-2013/>

¹²⁸ Obavještajci: ep. 307 - 13.03min

¹²⁹ <http://www.routerpasswords.com/>

Gibson & Joukowsky algoritam

U epizodi Obavještajaca središte radnje je algoritam za kodiranje datoteka koji su osmislili američki programeri Gibson i Joukowsky ¹³⁰. Prema objašnjenju iz serije, njihov algoritam – G&J algoritam – upotrebljava se za zaštitu elektroničkih aktivnosti na Internetu poput slanja elektroničke pošte ili kupovanja sadržaja preko Interneta. Navedeni algoritam u stvarnosti ne postoji, ali opisana svrha tog algoritma odgovara dvama postojećim sigurnosnim protokolima na Internetu – SSL-u i TLS-u.

Sloj osiguranih priključaka, (engl. *Secure Socket Layer* – SSL) i Sigurnost prijenosnog sloja (engl. *Transport Layer Security* – TLS) najkorišteniji su sigurnosni protokoli današnjice. Glavna svrha je osiguranje veze između računala na Internetu ili lokalne mreže. Neke od glavnih primjena protokola su zaštita transakcija kreditnih kartica, slanje i primanje elektroničke pošte te prijenos osjetljivih podataka na Internetu. Internetske stranice koje su zaštićene SSL i TLS protokolima označene su zelenom bojom i sadrže sliku lokota u URL adresi, a ponekad i ime pravnog vlasnika stranice. Također, stranica ne započinje s „http://“ i ne koristi standardni port 80, nego port 443 i započinje s „https://“ (engl. *Hypertext Transfer Protocol Secure*) ¹³¹.

Možemo zaključiti kako su za potrebe serije scenaristi naveli fiktivni algoritam umjesto stvarnog sigurnosnog protokola zbog potrebe radnje. Za razliku od G&J algoritma, tvorac SSL-a – dr. Taher Elgamal – je poznat u računalnoj industriji ¹³².

AES

U američkom filmu „Operacija *Swordfish*“ glavnom liku objašnjavaju kako je sustav u koji treba provaliti zaštićen 128 bitnom enkripcijom ¹³³. Sva današnja enkripcija temelji se na Naprednom enkripcijskom standardu (engl. *Advanced Encryption Standard* - AES). Za zaštitu podataka, AES upotrebljava specifični ključ kako bi kodirao i kasnije dekodirao sadržaj. Trenutni standard enkripcije je 128 bitni, tj. upotrebljava se ključ duljine 2^{32} bita, tj. 128 bita. U svrhu zaštite podataka ključ takve duljine je adekvatan, budući da pojedinačno računalo pristupom „grube sile“

¹³⁰ Obavještajci: ep. 307 - 30.52min

¹³¹ <https://www.globalsign.eu/ssl-information-center/what-is-ssl.html>

¹³² <http://www.forbes.com/profile/taher-elgamal/>

¹³³ Operacija *Swordfish*: 27.53min

(engl. *brute force*) enkripciju ne može provaliti u bilo kakvom praktičnom razdoblju ¹³⁴. Kao primjer se navodi analogija u kojoj sva današnja računala skupa ne bi mogla provjeriti više od 2^{75} ključeva godišnje, što je i dalje mnogo manji udio kombinacija od svih mogućih 2^{128} kombinacija AES-a ¹³⁵.

Međutim, u istom filmu kasnije susrećemo situaciju u kojoj se očekuje od glavnog lika da probije zaštitu s 512 bitnom enkripcijom, a pred kraj filma je navedena i 1024 bitna enkripcija ^{136 137}. U oba slučaja su navedene fiktivne enkripcije koje su mnogo veće od AES-ovog standarda. Različite organizacije od 2013. godine prelaze na 256 bitnu enkripciju, koja je dovoljna za bilo kakav oblik zaštite podataka – 512 i 1024 bitne varijante nisu niti realne niti praktične ¹³⁸.

Vernamova šifra

U istoj sceni u kojoj se spominje 512 bitna enkripcija, u Operaciji *Swordfish* navodi se Vernamova šifra ¹³⁹. Riječ je o postupku šifriranja jednokratnim ključem koji je izumio Gilbert Vernam te je u teoriji matematički neslomljiva. Jednokratni ključ sadrži u potpunosti nasumične podatke za kodiranje poruke i dolazi u dva primjerka – jedan za kodiranje, a drugi za dekodiranje poruke – te se smije upotrijebiti samo jednom ¹⁴⁰. U filmu također se spominje da se ključ uništava prilikom kodiranja. Budući da se u današnjem dobu takvi ključevi najčešće primjenjuju na računalima, pohranjeni su na različitim optičkim medijima ili USB memoriji. U tom slučaju savjetuje se uništavanje medija zato što se obrisani podatci lako mogu rekonstruirati i ponovno upotrijebiti ¹⁴¹.

Međutim, Vernamova šifra navedena u filmu opisana je prvo kao 128 bitna, a zatim kao 512 bitna. Vernamova šifra nikako ne može biti niti 128 bitna niti 512, budući da duljina njenog ključ nije uvjetovana AES-om, nego duljinom poruke koju treba kodirati. 128 bitna enkripcija ima ključ fiksne duljine 128 bita te se upotrebljava zbog lakše primjene nego Vernamova šifra čiji ključ mora biti duljine poruke i u

¹³⁴ <http://www.inet2000.com/public/encryption.htm>

¹³⁵ <http://blog.agilebits.com/2013/03/09/guess-why-were-moving-to-256-bit-aes-keys/>

¹³⁶ Operacija *Swordfish*: 35.45min

¹³⁷ Operacija *Swordfish*: 1.16.30h

¹³⁸ Parks, A, 13.str.

¹³⁹ Operacija *Swordfish*: 35.37min

¹⁴⁰ http://www.pro-technix.com/information/crypto/pages/vernam_base.html

¹⁴¹ http://www.ranum.com/security/computer_security/papers/otp-faq/

potpunosti nasumičan, tj. jedinstven. Iako je 128 bitni ključ teoretski moguće probiti, potrebna je velika količina vremena, dok je kodiranje jednostavnije od Vernama ¹⁴². Vernamova šifra se stoga upotrebljava za vrlo osjetljive podatke i nije toliko česta pojava, za razliku od standardne AES enkripcije.

5.3. Virusi

Virusi su prisutni u građi koja se posvećuje hakerima, osobito u kontekstu napada na osjetljive računalne sustave. Prema analiziranim primjerima prevladavaju stvarni virusi ili virusi koji se temelje na stvarnim podvrstama i funkcijama virusa. S obzirom na specifičnu funkciju virusa unutar radnje, primarno su prisutni u građi koja se fokusira na uporabu računalne tehnologije, uglavnom u protuzakonite svrhe.

Cookie Monster

U Hakerima možemo vidjeti virus „*Cookie Monster*“ ¹⁴³. Riječ je o fiktivnom virusu koji je referenca na računalni program koji je nastao 1970. godine te se smatra jednim od najranijih primjera ponašanja računalnih virusa. Program je bio aktivan među pozadinskim procesima računala te bi pod određenim uvjetima zaustavio programe koje korisnik upotrebljava i zatražio „kolačić“. Program bi prestao djelovati nakon što bi korisnik upisao „kolačić“ ¹⁴⁴. U nekim slučajevima je program imao mogućnost namještanja „budilice“ kad bi se program trebao pokrenuti i kad bi trebao završiti, stoga ga je bilo teško pronaći pretražujući aktivne programe ¹⁴⁵. Program se nije smatrao virusom, budući da se nije umnožavao niti širio po drugim računalima, ali ga se smatra pretečom virusa zbog onemogućavanja rada računala.

Zanimljiva je činjenica kako program nije napravljen prema liku „*Cookie Monster*“ (hrv. Keksomlat) iz serije „Ulica Sezam“, nego prema crtanom medvjedu iz reklame za žitarice iz 1960-ih godina ¹⁴⁶.

¹⁴² <http://cryptojedi.org/peter/data/notes-20111014.pdf>

¹⁴³ Hakeri: 1.25.48h

¹⁴⁴ <http://uanr.com/articles/virus.html>

¹⁴⁵ <http://www.multicians.org/cookie.html>

¹⁴⁶ http://content.time.com/time/specials/packages/article/0,28804,1839579_1839578_1839526,00.html

Rabbit virus

U Hakerima također možemo vidjeti kako jedan od glavnih likova upotrebljava „zečji virus“ kako bi onеспособio središnje računalo organizacije ¹⁴⁷. „Zečji virus“ (engl. *rabbit virus*) ili „bomba račvanja“ (engl. *fork bomb*) je vrsta virusa čija je svrha provesti napad uskraćivanja usluge (engl. *denial-of-service* – DoS). Ovakva vrsta virusa se množi kako bi zauzela resurse računala i onemogućili njegovo korištenje ¹⁴⁸. Ovakvi su se virusi prvi put pojavili 1974. godine pod nazivom *rabbit virus* ¹⁴⁹. Termin *fork bomb* upotrebljava se za vrstu virusa koji provode ovakve napade na sustavima temeljenima na Linuxu. Naziv dolazi od funkcije „fork()“ koja stvara novi proces iz postojećeg procesa, tj. konstantno stvara nove procese u sustavu ¹⁵⁰.

GPI i FSI virusi

Posljednji primjeri virusa koji se spominju u Hakerima su GPI i FSI virusi ¹⁵¹. Skraćenice stoje za *General Purpose Infector* (hrv. Infekcija opće namjene) i *File Specific Infector* (hrv. Infekcija specifične datoteke). GPI virus ima cilj pronaći i zaraziti sve izvršne datoteke na računalu kako bi ih onеспособio. FSI virus pokušava zaraziti određenu vrstu datoteka, s tim da se može prenijeti na druge datoteke kako bi zarazio ciljanu vrstu ^{152 153}.

Prema nekim izvorima viruse koji zaraze druge datoteke možemo smatrati „klasičnim“ oblikom virusa, kao i BSI (engl. *Boot Sector Infector* – Infekcija sektora pokretanja) virusi koji zaraze sektor pokretanja (engl. *boot sector*) računala i postaju prvi programi koji se pokreću prilikom pokretanja sustava i preuzimaju računalo ¹⁵⁴.

¹⁴⁷ Hakeri: 1.26.23h

¹⁴⁸ <http://www.cyberciti.biz/faq/understanding-bash-fork-bomb/>

¹⁴⁹ http://www.paretologic.com/resources/newsletter/viruses_a_history.aspx

¹⁵⁰ <http://www.unixguide.net/unix/programming/1.1.1.shtml>

¹⁵¹ Hakeri: 1.29.08h

¹⁵² <http://www.wonko.info/ipt/sei/soceth2.htm>

¹⁵³ Davendranath G. Jha, 70. str.

¹⁵⁴ https://www.virusbtn.com/resources/glossary/file_infector_virus.xml

Keystroke virus

U Obavještajcima glavni likovi spominju uporabu *keystroke* virusa iz 90-ih godina 20.-og stoljeća ¹⁵⁵. *Keystroke logger*, odnosno *keylogger* je vrsta programa koja prati i zapisuje što korisnik tipka kako bi podatke kasnije slao vlasniku programa. Unatoč tome što ovi programi sami po sebi nisu zloćudni – roditelji ih mogu upotrebljavati za praćene aktivnosti vlastite djece, a policija radi istrage – mogu se upotrebljavati u takve svrhe. U tom slučaju postoji rizik prikupljanja korisnikovih povjerljivih podataka poput lozinaka, brojeva računa i PIN-ova ¹⁵⁶.

Keyloggeri koji nisu svjesno instalirani na računalo šire se kao i drugi oblici *malwarea* – otvaranjem nepoznatih privitaka elektroničke pošte, društvenih mreža ili IM usluga. Moguće je prepoznati prisutnost *keyloggera* ako korisnik zamijeti sporije performanse prilikom pretraživanja Interneta, stanke u kretnji miša ili u tipkanju teksta te nepodudaranje tipkanog sadržaja na ekranu ¹⁵⁷.

5.4. Hidra

U Operaciji *Swordfish* glavnog lika unajme kako bi napravio specifičnu vrstu crva – „hidru“, crva s više glava ¹⁵⁸. Navedena podvrsta crva ustvari ne postoji te je izmišljena za potrebe filma. Crv pod nazivom „*Hydra*“ postoji, ali to je crv koji je programiran u *Visual Basicu* i širi se kao privitak u elektroničkoj pošti te zarazi sustav nakon što se privitak otvori ¹⁵⁹. Crv u filmu je opisan kao „višeglavi“ crv koji može pronaći „digitalne otiske“ na zaštićenoj mreži. Prema potonjem i navedenom stvarnom primjeru možemo zaključiti kako vrsta crva iz filma ustvari ne postoji.

5.5. Snifferi

U Obavještajcima i Operaciji *Swordfish* spominje se uporaba *sniffera* (hrv. njuškalo) ^{160 161}. *Sniffer* je program koji prati protok podataka na računalu koje je

¹⁵⁵ Obavještajci: ep. 410 - 38.22min

¹⁵⁶ <http://www.combofix.org/what-is-a-keylogger-virus-and-how-to-remove-it.php>

¹⁵⁷ <http://blogs.mcafee.com/consumer/what-is-a-keylogger>

¹⁵⁸ Operacija *Swordfish*: 35.29min

¹⁵⁹ <http://www.eset.com/us/threat-center/encyclopedia/threats/hydra/>

¹⁶⁰ Obavještajci: ep. 307 - 30.00min

¹⁶¹ Operacija *Swordfish*: ep. 34.53min

umreženo. Program kopira podatke koje prati, ali ih ne preusmjerava niti izmjenjuje. *Snifferi* su često u uporabi u legalne svrhe – mrežni inženjeri i administratori ih upotrebljavaju– ali ih također upotrebljavaju hakeri za proučavanje podataka na drugim računalima ¹⁶². Kako podatci korisnika ne bi bili izloženi *snifferima* preporučuje se zaštita osjetljivog sadržaja kodiranjem kako ne bi bili lako čitljivi ¹⁶³.

5.6. Botovi

U epizodi Obavještajaca informatički stručnjaci opisuju uporabu računala kao „roba“ (engl. *slave*) ¹⁶⁴. Unatoč tome što takav izraz nije često u uporabi, opisani koncept računala je moguć. Hakeri često upotrebljavaju programe koji se zovu „botovi“ – skraćeno od „robot“ – kako bi preuzeli računalo koje bot zarazi. Računalo koje haker preuzme zove se „zombi“ i upotrebljava ga u svrhe preuzimanja drugih računala, slanja *spama* ili za DDoS napade (engl. *Distributed Denial of Service*) ¹⁶⁵. Botove je teško otkriti, budući da su deaktivirani kad ih haker ne treba, a i nazivi im često sliče postojećim legitimnim programima. Bot je povezan s operativnim sustavom i pokreće se sa svakim paljenjem računala ¹⁶⁶. Iako se pretpostavlja da hakeri koji upotrebljavaju botove posjeduju napredno znanje o računalima, prema nekim izvorima je riječ o mladim hakerima koji nemaju iskustva u programiranju te upotrebljavaju tuđi kod. Stoga se za njih često upotrebljava izraz „*script kiddies*“ (hrv. „dječica programeri“) ¹⁶⁷. U slučaju otkrivanja napada potraga ne dovodi do hakera nego do zombija preko kojeg je napad napravljen.

Na uporabu botova možemo nadovezati scenu iz Puta prema dolje u kojoj se opisano kako je haker preuzeo više računala kako bi preko njih obavljao istu vrstu zadatka s različitih računala ¹⁶⁸. Skupina umreženih računala kojima upravljaju botovi naziva se „mreža botova“ (engl. *bot net*) ili „vojska zombija“ (engl. *zombie army*). Broj

¹⁶² http://compnetworking.about.com/od/networksecurityprivacy/g/bldef_sniffer.htm

¹⁶³ <http://www.symantec.com/connect/articles/sniffers-what-they-are-and-how-protect-yourself>

¹⁶⁴ Obavještajci: ep. 307 - 46.04min

¹⁶⁵ <http://us.norton.com/cybercrime-bots>

¹⁶⁶ http://netsecurity.about.com/od/frequentlyaskedquestions/qt/pr_bot.htm

¹⁶⁷ <http://computer.howstuffworks.com/zombie-computer1.htm>

¹⁶⁸ Put prema dolje: ep. 212 - 23.20min

računala u *botnetu* može varirati, od nekoliko stotina pa do nekoliko tisuća ili čak stotina tisuća, ovisno o količini zaraženih računala ¹⁶⁹.

5.7. Back door

U Operaciji *Swordfish* moguće je primijetiti uporabu riječi „*back door*“ i „*trap door*“ (hrv. stražnja vrata) kao i u filmu *Hakeri* ^{170 171 172}. Riječ je kodu koji programer može ostaviti u sustavu kako bi mu kasnije lakše mogao pristupiti za potrebe testiranja ¹⁷³. Ako se *back door* ne odstrani, može postati ozbiljan sigurnosni propust u sustavu. Često ih upotrebljavaju hakeri kako bi kasnije imali pristup sustavu u koji su provalili. *Back door* nije moguće pouzdano uočiti niti odstraniti, budući da skriva svoju prisutnost i nije moguće pratiti kad se netko preko njega prijavi u sustav. Jedini pouzdani način odstranjivanja *back doora* je formatiranjem cijelog sustava ¹⁷⁴.

5.8. Logička bomba i stražnja vrata

U istom filmu glavnom lika ispituju kako je uspio provaliti u sustav Ministarstva obrane, a jedan od odgovora je da je „bacio *logic bomb* u *trap door*“ ¹⁷⁵. *Logic bomb* (hrv. logička bomba) je mali program ili dio programa koji provodi svoju funkciju kad su postignuti uvjeti pod kojima se aktivira. Funkcija programa može biti raznolika, od brisanja datoteka, izmjene koda ili izmjena u operativnom sustavu. Logičke bombe najčešće ostavljaju pojedinci koji imaju pristup sustavu, bilo ovlašteni ili neovlašteni ¹⁷⁶. *Trap door* je drugi naziv za *back door* koji smo pojasnili u odlomku prije.

Međutim, dijalog scene ne funkcionira iz nekoliko razloga. Glavni lik nije mogao upotrijebiti niti logičku bombu niti stražnja vrata kao što je objašnjeno, budući da nije imao pristup Ministarstvu obrane. Tek je pokušavao dobiti pristup sustavu, a bombu ili vrata je moguće primijeniti samo ako korisnik već ima pristup sustavu.

¹⁶⁹ <http://searchsecurity.techtarget.com/definition/botnet>

¹⁷⁰ Operacija *Swordfish*: 34.41min

¹⁷¹ Operacija *Swordfish*: 1.17.28h

¹⁷² *Hakeri*: 25.15min

¹⁷³ <http://www.sans.edu/research/security-laboratory/article/log-bmb-trp-door>

¹⁷⁴ http://www.linuxsecurity.com/resource_files/documentation/hacking-dict.html#back-door

¹⁷⁵ Operacija *Swordfish*: 34.41min

¹⁷⁶ <http://www.sans.edu/research/security-laboratory/article/log-bmb-trp-door>

Logička bomba također ne bi imala smisla u takvoj situaciji zato što njeni uvjeti ne bi bili postignuti u kratkom vremenu od 60 sekundi – koje je bilo zadano u sceni prije – a ipak je logička bomba „bomba“. Namjena logičke bombe jest da ona miruje duže vrijeme dok se njeni uvjeti ne ispune. Dakle, možemo pretpostaviti kako je opis u sceni u potpunosti netočan, odnosno da scenaristi jesu bili upoznati s izrazima, ali nisu bili upoznati s njihovim tehničkim značenjem i stvarnom funkcijom.

5.9. Hardversko hakiranje

U epizodi Obavještajaca se navodi kako računala tvrtke koju promatraju nisu spojena na Internet te ih zato nije moguće hakirati ¹⁷⁷. Samo zato što računalo nema pristup Internetu ne znači da hakeri nemaju pristup njemu. Primjer toga možemo naći u virusu *Stuxnet*.

Stuxnet je virus koji je bio dizajniran kako bi kroz period od nekoliko mjeseci pronašao specifično računalo. To računalo je bilo u iranskom postrojenju za obogaćivanje uranija. Virus se prenosio pomoću USB memorije, nakon čega se širio po postrojenju tražeći računalo zaduženo za regulaciju nuklearnih centrifuga. Virus je povećao brzinu vrtnje centrifuga te slao lažne informacije kako bi izgledalo da sustav normalno funkcionira. Pretpostavlja se da je da je oko 1000 centrifuga trebalo biti zamijenjeno u postrojenju Natanz zbog napada 2010. Godine ¹⁷⁸.

Mogućnost hakiranja također dolazi kod uporabe radio valova. Navodi se kako se povećava uporaba radio valova za komunikaciju među postrojenjima, što također dovodi do rizika od presretanja komunikacije. Još jedan način hakiranja koji ne zahtjeva prisutnost Interneta, ali je mnogo kompliciraniji za provesti, jest hardversko hakiranje, tj. hardverski Trojanci. U tom slučaju se hakiranje provodi preko modificiranja elektroničkih komponenti. Najčešće se provodi u fazi proizvodnje. Iako se konačni proizvodi testiraju kako bi se uočile izmjene, u nekim slučajevima je količina mogućih izmjena prevelika. Postoje određene preventivne mjere poput povjeravanja dizajniranja i proizvodnje pouzdanim tvrtkama i ljudima kako ne bi došlo

¹⁷⁷ Obavještajci: ep. 307 - 12.24min

¹⁷⁸ Nicol, David M.: Hacking the Lights Out

do sabotaze u ranim stadijima. Također, u nekim proizvodima upotrebljavaju se sigurnosni sklopovi za prepoznavanje napada i smanjivanje štete na minimum ¹⁷⁹.

Prema navedenoj sceni iz serije možemo pretpostaviti kako bi bilo vjerojatnije hakiranje pomoću prijenosne memorije, nego preko hardverskog hakiranja zato što potonje iziskuje dugoročnije planiranje. Budući da je epizoda emitirana 2004. godine, a uporaba virusa *Stuxnet* je zabilježena 2010. Godine, moguće je da su u doba emitiranja takve vrste napada bile manje vjerojatne nego danas.

6. HARDVER

S obzirom da su računalne komponente, tj. hardver često jedini fizički primjer informatike u popularnoj kulturi, moguća je mnogo veća fizička prisutnost unutar sadržaja. Vjernost varira ovisno o potrebi radnje, a i prisutnosti tehničkih savjetnika. Kod nekih primjera može se uočiti vjernost u opisu i tehničkim karakteristikama u uporabi hardvera. Unatoč stručnjacima za savjetovanje, neki primjeri umjesto tehničke preciznosti prikazuju nedosljednost u opisima i uporabu tehnologije koja se ne podudara s njenom stvarnom primjenom. U drugim slučajevima možemo primijetiti uporabu stvarne tehnologije u nepraktične svrhe, ukazujući na manjak stručnosti savjetnika, ako su uopće bili prisutni.

6.1. Dial-up

Na početku *Hakera* možemo vidjeti kako glavni lik pristupa Internetu. Spominje se kako je spojio računalno na telefon ¹⁸⁰. Film je snimljen u doba *dial-upa* kad se Internetu pristupalo putem običnih telefonskih linija. Za spajanje na Internet bilo je potrebno posjedovati modem i aktivnu telefonsku liniju na koju je moguće spojiti se. Sam naziv pristupa (engl. *dial-up* – hrv. biranje broja) dolazi od činjenice da modem

¹⁷⁹ Villasenor, John: *The Hacker in Your Hardware*

¹⁸⁰ *Hakeri*: 9.36min

„bira broj“ za uspostavu poziva kako bi se uspostavila veza s pružateljem Internet usluga (engl. *Internet service provider* - ISP). Za vrijeme uporabe *dial-up*, telefonska linija je zauzeta, tj. nije moguće upotrebljavati liniju za obično zvanje. Zbog navedene zauzetosti linije, a i same sporosti uporabe usluge – prosječna brzina pristupa Internetu je 56 kbit/s – *dial-up* se danas vrlo rijetko koristi, budući da ga je naslijedila usluga širokopojasnog Interneta koja omogućava mnogo veću brzinu pristupa Internetu bez ograničavanja uporabe obične telefonske linije ¹⁸¹.

6.2. Superračunala, William Gibson i *heavy metal*

Nešto kasnije u istom filmu spominju se tzv. superračunala ¹⁸². Riječ je računalima koja obavljaju procese mnogo brže od prosječnih računala u svakodnevnoj uporabi. Neki od kriterija za superračunala su da upotrebljavaju više od jednog CPU-a za izvršavanje zadaća, imaju ogromnu količinu prostora za pohranu kako bi mogli provoditi više zadataka istovremeno te imaju mogućnost izračunavanja vektorske aritmetike, tj. mogu izračunavati više slijedova operacija odjednom ¹⁸³. Također imaju posebne sustave klimatizacije kako ne bi došlo do pregrijavanja. Operativni sustavi koje upotrebljava većina superračunala su Linux ili Unix zbog njihove stabilnosti i fleksibilnosti. Uglavnom se upotrebljavaju za znanstvene izračune, ali i za probijanje šifri te igranje šaha ¹⁸⁴. Jedni od najpoznatijih superračunala su *Deep Blue*, *Sequoia*, *Watson* i *Roadrunner* ¹⁸⁵.

Superračunalo navedeno u filmu – Gibson – je fiktivno ¹⁸⁶. Nazvano je prema američkom piscu Williamu Gibsonu koga se smatra ocem *cyberpunka* ¹⁸⁷. Glavni motivi žanra su prisutnost i utjecaj moderne tehnologije na društvo i pojedinca te način na koji se ljudi nose s vlastitom ulogom u modernom društvu. Osim tih motiva, glavnu ulogu u njegovim knjigama često imaju hakeri i utjecaj hakerske kulture, zbog čega je superračunalo i prozvano po njemu.

¹⁸¹ <http://www.buzzle.com/articles/broadband-vs-dial-up-connection.html>

¹⁸² Hakeri: 25.06min

¹⁸³ <http://computer.howstuffworks.com/supercomputers-used-for.htm>

¹⁸⁴ <http://www.wisegeek.org/what-is-a-supercomputer.htm>

¹⁸⁵ <http://whatis.techtarget.com/definition/supercomputer>

¹⁸⁶ Hakeri: 25.02min

¹⁸⁷ <http://web.archive.org/web/20120722083618/http://www.empmuseum.org/exhibitions/index.asp?articleID=1282>

U istoj sceni glavni likovi superračunalo opisuju kao „*heavy metal*“ (hrv. teški metal)¹⁸⁸. Superračunala i glavna računala se u hakerskom žargonu najčešće opisuju izrazima „*heavy metal*“ ili „*big iron*“ (hrv. veliko željezo). Pretpostavlja se da izrazi potječu iz činjenice da su glavna računala bila smještena u ogromnim metalnih okvirima veličine soba^{189 190}. *Heavy metal* je možda upotrijebljen radi „ozbiljnijeg“ prizvuka nego *big iron*.

6.3. Oštećenje podataka

U kasnijoj sceni spominje se kako je tvrdi disk s računala koje je upotrebljavao jedan od glavnih likova „neoštećen“ (engl. *uncorrupted*)¹⁹¹. Oštećenje podataka (engl. *data corruption*) je bilo kakav oblik štete ili grešaka koje se mogu pojaviti prilikom pohranjivanja podataka na računalu. Postoji nekoliko načina kako prepoznati oštećenje – nemogućnost otvaranja ili brisanja datoteka i direktorija, drukčija lokacija istih ili sporost pristupa tvrdom disku. Uzroci mogu biti hardverse, softverske ili ljudske naravi.

Tvrdi diskovi imaju pomične dijelove koji se s vremenom mogu istrošiti što skoro uvijek dovodi do oštećenja podataka koji su na njima pohranjeni. Programi također mogu biti odgovorni zato što loše napisani programi – često besplatni programi s Interneta – mogu uzrokovati nestabilnosti u radu računala i do pada sustava čime se mogu izgubiti vrijedni podatci. Programi poput *malwarea* mogu imati zadaću oštećivanja podataka, no takva uporaba je namjerna. Uzrok mogu biti i sami korisnici koji ne znaju pravilo rukovati računalom, npr. kod pravilnog gašenja sustava^{192 193}.

U sceni u kojoj se spominje neoštećenost tvrdog diska, možemo pretpostaviti da se referiralo na oštećenja koja je namjerno mogao izazvati korisnik, npr. uporabom *malwarea* za oštećivanje podataka ili namjernim mehaničkim oštećenjem tvrdog diska.

¹⁸⁸ Hakeri: 25.15min

¹⁸⁹ <http://www.cyberciti.biz/faq/bigiron-unix-systems/>

¹⁹⁰ <http://searchdatacenter.techtarget.com/definition/mainframe>

¹⁹¹ Hakeri: 33.01min

¹⁹² http://www.datarecovery.com.sg/data_recovery/data_corruption.htm

¹⁹³ <http://www.wisageek.com/what-is-data-corruption.htm>

6.4. Aktivna matrica

Prilikom opisa prijenosnog računala jednog od glavnih likova možemo čuti opis njegovih fizičkih karakteristika. Za početak se spominje da računalo ima ekran s „aktivnom matricom“ ¹⁹⁴. Aktivna matrica (engl. *active matrix*) je način izrade koji se upotrebljava za ekrane prijenosnih računala. Za razliku od pasivne matrice (engl. *passive matrix*) kod aktivne matrice svakom pikselu na ekranu dodijeljen je jedan tranzistor. Temelji se na tehnologiji tankoslojnih tranzistora (engl. *thin-film transistor*) te omogućava mnogo bolji kontrast boja i odziv prilikom promjena na ekranu ^{195 196}.

Prema sceni u filmu je prijenosno računalo s aktivnom matricom novitet i tehnološki fascinantno. S obzirom kada je film snimljen možemo pretpostaviti da je i bilo napredno 1995. godine s obzirom da je izrada LCD ekrana s aktivnom matricom u današnjem dobu norma za prijenosna računala i za druge primjene.

6.5. Višestruki ekrani i DS3 veza

U sceni Operacije *Swordfish* glavnom liku objašnjavaju kako sustav više ekrana i upotrebljava DS3 vezu za spajanje na Internet te se može spojiti na sedam mreža istovremeno ¹⁹⁷. Računalni sustavi s više ekrana najčešće upotrebljavaju dizajneri zbog povećanja produktivnosti. Prednosti više ekrana su mogućnost uporabe više programa odjednom, prijenos podataka između više programa te radi lakše usporedbe rezultata ¹⁹⁸. DS3 je internetska veza koja omogućava prijenos podataka do 45 Mb/s. DS3 vezu najčešće upotrebljavaju korporacije i sveučilišta s velikom količinom internetskog prometa ¹⁹⁹. Ova vrsta veze se primarno upotrebljava u SAD-u te se također zove T3 vezom, dok je europska varijanta E3 veza koja doseže maksimalnu brzinu od 34 Mb/s ²⁰⁰.

U kontekstu radnje računalo s ovakvim karakteristikama ne bi bilo praktično. Budući da glavni lik mora stvoriti crva u jednom programu, dakle i u jednom

¹⁹⁴ Hakeri: 46.37min

¹⁹⁵ <http://electronics.howstuffworks.com/lcd4.htm>

¹⁹⁶ <http://whatis.techtarget.com/definition/thin-film-transistor-TFT>

¹⁹⁷ Operacija *Swordfish*: ep. 36.25min

¹⁹⁸ <http://www.webdesignerdepot.com/2009/05/advantages-and-disadvantages-of-working-with-multiple-screens/>

¹⁹⁹ <http://ezinearticles.com/?Whats-the-Difference-Between-DS3-and-T3-Bandwidth?&id=94209>

²⁰⁰ <http://www.ad-net.com.tw/index.php?id=499>

programskom jeziku, računalo s više ekrana ne bi trebalo biti potrebno. Štoviše, bilo bi nepraktično zbog odvrćanja pozornosti i smanjenja produktivnosti. Daljnje scene u filmu potvrđuju to jer je prikazana izrada crva u samo jednom programu. DS3 veza je također suvišna jer je predviđena za tvrtke i za prijenos velike količine podataka poput video zapisa i ogromnih baza podataka. Dodatna nelogičnost u sceni je spominjanje „sedam različitih mreža“ zato što nije specificirano o kakvim je točno mrežama riječ. Čak ako se referiralo na umrežena korporativna računala, širokopojasne veze poput DS3 trebale bi biti ograničene brzinom prijenosa podataka prilikom pristupa, a ne brojem „mreža“ kojima se pokušava pristupiti. Možemo stoga pretpostaviti kako su termini upotrijebljeni bez predznanja o njihovoj namjeni.

6.6. 28.8 bps modem i P6 procesori

U Hakerima se glavni likovi dive prijenosnom računalu kolegice i komentiraju kako ima modem brzine 28,8 bps ²⁰¹. Kao što smo prije spomenuli, modemi u doba *dial-upa* povezivali su se na Internet putem telefonske linije. Maksimalna brzina koju je bilo moguće postići na klasičnom *dial-up* modemu bila je 56 kbps, tj. 56 kilobita po sekundi ²⁰². 1995. godine – godine snimanja Hakeri – najveća moguća brzina bila je 28.8 kbps ²⁰³. Lako je za zaključiti kako je napravljena očita pogreška u govoru. Glavni lik Phreak je naveo da modem na prijenosnom računalu ima brzinu „28.8 bps“ umjesto „28,8 kbps“. Bilo da je riječ o pogrešci u scenariju ili u trenutku izgovora, navedena brzina modema je tisuću puta manja od standarda. Čak i u doba snimanja filma je ovakva tehnička greška bila očita, osobito među upućenijim gledateljima.

U kasnijoj sceni glavni lik opisuje kako isto prijenosno računalo ima P6 integrirani sklop koji je trostruko brži od Pentiuma ²⁰⁴. Arhitektura P6 serije mikroprocesora bila je nasljednik Intelovog Pentiuma. Prvi mikroprocesor u P6 seriji bio je Pentium Pro te je izdan 1995. godine ²⁰⁵. Prema Intelovoj dokumentaciji prvi P6 procesor nije bio trostruko brži od Pentiuma, nego dvostruko ²⁰⁶. Opis se nastavlja te

²⁰¹ Hakeri: 46.37min

²⁰² <http://www.wisageek.org/what-is-a-modem.htm>

²⁰³ <http://compnetworking.about.com/library/weekly/aa112100a.htm>

²⁰⁴ Hakeri: 50.45min

²⁰⁵ <http://www.quepublishing.com/articles/article.aspx?p=482324&seqNum=17>

²⁰⁶ http://cdn.preterhuman.net/texts/computing/intel_cpu_datasheets/P6%20Performance.pdf

je navedeno kako prijenosno računalo ima PCI sabirnicu ²⁰⁷. Prema tehničkim karakteristikama Intelova serija P5 iz 1993. godine već je imala PCI sabirnicu ^{208 209}. Stoga je opis već implementirane tehnologije nelogičan i suvišan. Dalje je navedeno kako P6 upotrebljava RISC arhitekturu unatoč tome što ta serija mikroprocesora ustvari upotrebljava CISC arhitekturu ^{210 211}. Unatoč prisutnosti tehničkih stručnjaka, većina opisa tehničkih karakteristika tadašnjih prijenosnih računala je netočna.

6.7. Kloniranje

U epizodi Žice glavni likovi opisuju kako su uspjeli klonirati računalo kako bi mogli pratiti što osumnjičenici rade na računalu ²¹². Pojam kloniranja (engl. *cloning*) postoji u informatici, ali se ne odnosi na praćenje rada nekog računala, nego na kopiranje njegovog sadržaja. Kloniranjem se kopira sadržaj tvrdog diska kako bi se podatci mogli prenijeti na drugo računalo ili u svrhu sigurnosne kopije sustava ²¹³. U svrhu praćenja rada na računalu stoga se ne može upotrijebiti kloniranje, nego se moraju upotrijebiti određene vrste *malwarea*, odnosno *spywarea* za praćenje aktivnosti.

7. INFORMATIČKE REFERENCE

Uz različite primjere koji se tiču konkretne informatičke tehnologije, u građi možemo uočiti i spomen povijesnih aspekata računalstva i njegove aktivne primjene. U proučenoj građi ovakve reference su primarno bile uvjetovane prisutnošću tehničkih savjetnika i upućenošću ostatka osoblja u informatičku kulturu i povijest. Reference su se ticale povijesnog razvoja računala, hakerske kulture i književnosti

²⁰⁷ Hakeri: 50.50min

²⁰⁸ <http://www.pcguide.com/ref/cpu/fam/g5P54-c.html>

²⁰⁹ <http://www.karbosguide.com/hardware/module2d04.htm>

²¹⁰ Hakeri: 50.56min

²¹¹ <http://archive.arstechnica.com/cpu/4q99/risc-cisc/rvc-6.html>

²¹² Žica: ep. 206 - 48.36min

²¹³ <http://www.wisageek.com/what-is-disk-cloning.htm>

koja se doticala tematike hakera u društvu. Reference su stoga prikladne, budući da su analizirani primjeri pronađeni u građi čija su glavna tematika upravo hakeri i njihova kultura.

7.1. Hakerski nadimci

U Hakerima možemo vidjeti primjere različitih nadimaka za hakere ²¹⁴. Hakerski nadimci (engl. *handle*) su pseudonimi pod kojima hakeri djeluju i često se razlikuju od njihovih stvarnih ličnosti ²¹⁵. Hakeri ne biraju vlastite nadimke, nego im se dodjeljuju po njihovoj prikladnosti. Mnogo su prihvatljiviji „skromniji“ nadimci od samostalno dodijeljenih koji privlače pažnju – često se smatraju amaterskima ²¹⁶. Prema navedenome donekle je moguće analizirati nadimke iz filma.

Zero Cool – početnik koji se otpočетка smatrao vrhunskim, ali je ubrzo otkriven. *Crash Override* – haker koji nakon sudske zabrane ponovno počinje djelovati. *Acid Burn* – haker asocijalnog i agresivnog ponašanja s kojim treba oprezno rukovati. *The Phantom Phreak* – dotad neuhvaćeni haker koji je iskusan u manipuliranju telekomunikacijama. *Cereal Killer* – haker poznat po svojoj proždrljivosti. *Lord Nikon* – haker poznat po svojem pamćenju i iskustvu. *The Plague* – haker koji je sam odabrao nadimak, opisuje njegov karakter i sposobnosti te je na kraju uhićen.

Zanimljiva je činjenica kako je pravo ime *Cereal Killera* u filmu Emmanuel Goldstein što je pseudonim stvarnog hakera Erica Corleyja koji je istovremeno bio tehnički savjetnik za film ²¹⁷. Corleyjev nadimak – preuzet iz Orwellove 1984.-te – opisuje omraženog buntovnika ²¹⁸. S obzirom da je Corley poznat po sporovima oko probijanja zaštite filmske industrije i kršenja autorskih prava, nadimak je prikladan ²¹⁹.

²¹⁴ Hakeri: 14.40min

²¹⁵ http://www.linuxsecurity.com/resource_files/documentation/hacking-dict.html#handle

²¹⁶ <http://www.catb.org/jargon/html/H/handle.html>

²¹⁷ Hakeri: 21.16min

²¹⁸ <http://insecure.org/stf/hackenc.txt>

²¹⁹ <http://www.toptenz.net/top-10-infamous-hackers.php>

7.2. Savjest hakera

U jednoj sceni policajac naglas čita tekst o društvenom cilju hakera ²²⁰. Citirani tekst je napisao haker *The Mentor* pod nazivom Savjest hakera (engl. *The Conscience of a Hacker*) 1986. godine ²²¹. U filmu možemo čuti parafrazirano čitanje zadnja tri odlomka teksta o etičkim načelima hakera te kako ih svijet i vlasti gledaju i definiraju kao kriminalce.

7.3. Keyboard cowboy

Jedan od likova u *Hakerima* opisuje hakere kao „kauboje tipkovnice“ (engl. *keyboard cowboys*) ²²². Riječ je o izrazu kojim se slikovito opisivalo hakere u djelima Willama Gibsona ²²³. Naziv navjerojatnije asocira na pustolove koji djeluju na rubnim područjima mreže i civilizacije, osobito jer hakeri i u današnjem dobu djeluju izvan zakona.

7.4. Zakon o računalnom kriminalu

Prilikom uhićenja jednog od glavnih likova možemo čuti spomen „zakona o računalnoj prijevari i zlouporabi iz 1986. godine“ (engl. *computer fraud and abuse act*) ²²⁴. Riječ je o stvarnom zakonu u zakonodavstvu SAD-a prema kojem se pristup zaštićenom računalu bez ispravnog odobrenja smatra kaznenim djelom. Nakon izvornog donošenja zakona napravljene su dodatne izmjene kako bi se ograničila primjena na nezakonite aktivnosti ²²⁵.

7.5. Charles Babbage

Pri kraju filma glavni negativac putuje pod pseudonimom „Babbage“ ²²⁶. Pseudonim je referenca na engleskog matematičara Charlesa Babbagea čiji je

²²⁰ *Hakeri*: 38.05min

²²¹ <http://phrack.org/issues/7/3.html>

²²² *Hakeri*: 57.52min

²²³ http://www.nadir.org/nadir/archiv/Kultur/CyberPunk/whatis_cyberspace.article.html

²²⁴ *Hakeri*: 1.00.40min

²²⁵ <http://searchcompliance.techtarget.com/definition/The-Computer-Fraud-and-Abuse-Act-CFAA>

²²⁶ *Hakeri* 1.37.45

diferencijalni stroj bio poznat po tome što je mogao rješavati matematičke izračune. Zbog funkcije stroja Babbagea se danas smatra „ocem“ računalstva ²²⁷.

7.6. 2600

Na početku Mreže glavni lik odjavljuje pretplatu za časopis „2600“ ²²⁸. 2600 je informatički časopis koji se primarno posvećuje računalnoj tehnologiji i hakiranju ²²⁹. Urednik časopisa je prije spomenuti Eric Corley, također poznat i kao Emmanuel Goldstein.

²²⁷ <http://www.cbi.umn.edu/about/babbage.html>

²²⁸ Mreža 13.33

²²⁹ <http://www.barnesandnoble.com/w/2600-magazine-2600-magazine/1115893352?ean=2940016773599>

²³⁰ <http://www.2600.com/>

ZAKLJUČAK

Analizirajući različite oblike medija primijetili smo veliku zastupljenost informatike u današnjoj popularnoj kulturi. 90-ih godina 20.-tog stoljeća računalstvo nije bilo toliko razvijeno, a uporaba osobnih računala nije bila toliko proširena kao danas, stoga je bilo zastupljeno primarno u građi kojoj je glavni fokus bio računalstvo. Sa sve većom prisutnošću računala i povećanjem njihovih korisnika počela je rasti i informatička osviještenost, a time i njena prisutnost u popularnoj kulturi. Dodatni razlog veće zastupljenosti informatike može biti nagli razvoj Interneta krajem 20.-tog stoljeća, što je dovelo do veće povezanosti i informiranosti korisnika. S obzirom na stalni razvoj i širenje Interneta i informatičke kulture, možemo očekivati sve veću prisutnost informatike u popularnoj kulturi – bez obzira je li relevantna za radnju ili ne.

Preciznost informacija u građi primarno ovisi o tome je li informatika u središtu radnje i utječe li na nju. Unatoč tome, u nekim slučajevima kad su glavni fokus radnje uočeni primjeri temelje se na pogrešnim informacijama i primjeni u kontekstu radnje. Stoga možemo zaključiti kako ustrajnost za preciznošću može varirati između različitih slučajeva. Također, preciznost kad informatika nije u središtu radnje također ovisi o pristupu tvoraca. Uočena je veća točnost u prikazu informatike kad su prisutni informatički stručnjaci u ulozi savjetnika. Kod njihove prisutnosti također možemo primijetiti i više manjih referenci na računalnu kulturu, ali ponekad dolazi i do netočnosti unatoč njihovom stručnosti.

Ako uzmemo u obzir omjer točnog prikaza informatike u odnosu na netočne, većina primjera demonstrira informiranost pri uprizorenju informatičke kulture, osobito u primjerima koji su nastali u zadnjih 10 godina. Dok je ranije bila moguća manja preciznost i vjernost, možemo pretpostaviti kako u današnjem dobu informatička pismenost uvelike utječe na percepciju promatrača. Daljnja istraživanja će pokazati kojim tijekom će ići prikaz informatike. Mediji moraju biti spremni na obrazovanost i sve veću tehnološku osviještenost pojedinca u daljnjem razvoju društva. Što će više popularna kultura asimilirati informatiku i sve njene aspekte, to će njena percepcija biti preciznija i vjernija struci – što također dovodi i do moguće obrazovne funkcije što je popularna kultura vjernija strukama koje navodi.

REFERENTNA GRAĐA

- „About Digital Book World“. *Digital Book World*. F+W Media Inc. n.d. Internet. 29.9.2014. <<http://www.digitalbookworld.com/join/about/>>
- „Advantages and Disadvantages of Working with Multiple Screens“. *WebDesignerDepot.com*. 11.5.2009. Internet. 30.9.2014. <<http://www.webdesignerdepot.com/2009/05/advantages-and-disadvantages-of-working-with-multiple-screens/>>
- „Advertising and the BBC Brand“. *BBC*. n.d. Internet. 29.9.2014. <<http://www.bbc.co.uk/editorialguidelines/page/guidelines-editorial-integrity-advertising/>>
- „back door“. *Hacking Lexikon*. 21.8.2000. Internet. 30.9.2014. <http://www.linuxsecurity.com/resource_files/documentation/hacking-dict.html#back-door>
- „Backgammon Online“. *Backgammononline Inc.* n.d. Internet. 29.9.2014. <<http://backgammononline.com/>>
- „Call of Duty: World at War“. *Wikia inc.* n.d. Internet. 29.9.2014. <http://callofduty.wikia.com/wiki/Call_of_Duty:_World_at_War>
- „Computer Passwords“. *Computer Hope*. n.d. Internet. 30.9.2014. <<http://www.computerhope.com/issues/ch000300.htm>>
- „Computer Viruses“. *Wonko.info*. n.d. Internet. 30.9.2014. <<http://www.wonko.info/ipt/sei/soceth2.htm>>
- „Cryptology and Data Secrecy: The Vernam Cypher“. *Protechnix*. n.d. Internet. 30.9.2014. <http://www.pro-technix.com/information/crypto/pages/vernam_base.html>
- „Data Corruption“. *DataRecovery.com.sg*. n.d. Internet. 30.9.2014. <http://www.datarecovery.com.sg/data_recovery/data_corruption.htm>
- „Encryption“. *Inet2000.com*. n.d. Internet. 30.9.2014. <<http://www.inet2000.com/public/encryption.htm>>
- „Everything you Need to Know About #Hashtags on Facebook“. *Social Bakers*. n.d. Internet. 29.9.2014. <<http://www.socialbakers.com/blog/1826-everything-you-need-to-know-about-hashtags-on-facebook>>
- „Facial recognition“. *FindBiometrics*. TopickZ inc. n.d. Internet. 29.9.2014. <<http://findbiometrics.com/solutions/facial-recognition/>>
- „File infector virus“. *Virus Bulletin*. n.d. Internet. 30.9.2014. <https://www.virusbtn.com/resources/glossary/file_infector_virus.xml>
- „FlashPeak SlimBrowser“. *SlimBrowser*. FlashPeak Inc. n.d. Internet. 29.9.2014. <<http://www.slimbrowser.net/en/webhelp/index.htm>>
- „Handle“. *Hacking Lexikon*. n.d. Internet. 30.9.2014. <http://www.linuxsecurity.com/resource_files/documentation/hacking-dict.html#handle>

- „Handle“. *The Jargon File*. n.d. Internet. 30.9.2014. <<http://www.catb.org/jargon/html/H/handle.html>>
- „How do you hide your IP address?“. *HowStuffWorks*. InfoSpace LLC. 20.5.2011. Internet. 29.9.2014. <<http://computer.howstuffworks.com/internet/basics/hide-ip-address.htm>>
- „How Image Enhancement Work in Real Life“. *Asmag.com*. Messe Frankfurt New Era Business Media Ltd. 28.3.2012. Internet. 29.9.2014. <<http://www.asmag.com/showpost/12849.aspx>>
- „IMAP“. *What Is My IP Address*. n.d. Internet. 29.9.2014. <<http://whatismyipaddress.com/imap>>
- „Intel Pentium („P5“/ „P54C“)“. *The PC Guide*. 17.4.2001. Internet. 30.9.2014. <<http://www.pcguide.com/ref/cpu/fam/g5P54-c.html>>
- „Left 4 Dead“. *Wikia inc*. n.d. Internet. 29.9.2014. <http://left4dead.wikia.com/wiki/Left_4_Dead>
- „Mail Server“. *What Is My IP Address*. n.d. Internet. 29.9.2014. <<http://whatismyipaddress.com/mail-server>>
- „MyShout“. *MyShout*. n.d. Internet. 29.9.2014. <<http://www.myshout.com.au/#shouthappy>>
- „mySHOUT.US“. *AMC TV*. n.d. Internet. 29.9.2014. <http://media.amctv.com/img/originals/breakingbad/myshout/pinkman_page.html>
- „NAT“. *What Is My IP Address*. n.d. Internet. 29.9.2014. <<http://whatismyipaddress.com/nat>>
- „Passenger Convenience Innovations: The Internet“. *Alaska Airlines*. Alaska Air Group Inc. 8.2014. Internet. 29.9.2014. <<http://www.alaskaair.com/content/about-us/newsroom/technology.aspx>>
- „POP3“. *What Is My IP Address*, 2014. 29.9.2014. <<http://whatismyipaddress.com/pop3>>
- „Primetime“. *FX Canada*. Rogers Media. n.d. Internet. 29.9.2014. <<http://www.fxnowcanada.ca/shows/>>
- „Proxy poslužitelji“. *Hrvatska akademska i istraživačka mreža*. 8.2010. Internet. 29.9.2014. <<http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-08-309.pdf>>
- „P6 Performance“. *Intel Corporation*. 1995. Internet. 30.9.2014. <http://cdn.preterhuman.net/texts/computing/intel_cpu_datasheets/P6%20Performance.pdf>
- „Resident Evil 4“. *Wikia inc*. n.d. Internet. 29.9.2014. <http://residentevil.wikia.com/Resident_Evil_4>
- *RouterPasswords.com*. n.d. Internet. 30.9.2014. <<http://www.routerpasswords.com/>>

- „Search-Wise.net“. *Compuhire*. n.d. Internet. 29.9.2014. <<http://search-wise.net/>>
- „SG World Introduces Text-to-Speech: An innovative, virtual world featuring TTS voice for global English chat“. *MyNewsDesk*. NHST. 11.7.2012. Internet. 29.9.2014. <<http://www.mynewsdesk.com/jp/pressreleases/sg-world-introduces-text-to-speech-an-innovative-virtual-world-featuring-tts-voice-for-global-english-chat-779340>>
- „Taher Elgamal“. *Forbes.com*. n.d. Internet. 30.9.2014. <<http://www.forbes.com/profile/taher-elgamal/>>
- „The most common passwords used online in the last year revealed (and 'password' STILL tops the list)“. 25.10.2012. Internet. 30.9.2014. <<http://www.dailymail.co.uk/sciencetech/article-2223197/Revealed-The-common-passwords-used-online-year-password-STILL-tops-list.html>>
- „The Opera Group“. *Opera Software*. 2014. Internet. 29.9.2014. <<http://www.operasoftware.com/company>>
- „The Safari Browser“. *W3Schools*. Refsnes Data. n.d. Internet. 29.9.2014. <http://www.w3schools.com/browsers/browsers_safari.asp>
- „The World In An Eye“. *Department of Computer Science*. Columbia University. n.d. Internet. 30.9.2014. <http://www1.cs.columbia.edu/CAVE/projects/world_eye/>
- „Understanding Bash fork() Bomb ~:(){ :|:& };:“. *nixCraft*. 2.9.2012. Internet. 30.9.2014. <<http://www.cyberciti.biz/faq/understanding-bash-fork-bomb/>>
- „What's a Bot?“. *Symantec Corporation*. n.d. Internet. 30.9.2014. <<http://us.norton.com/cybercrime-bots>>
- „What's changing on the BBC website?“. *BBC*. 29.9.2014. Internet. 29.9.2014. <<http://www.bbc.co.uk/bbc.com/faq/>>
- „What Is A Keylogger Virus And How To Remove It“. *ComboFix*. n.d. Internet. 30.9.2014. <<http://www.combofix.org/what-is-a-keylogger-virus-and-how-to-remove-it.php>>
- „What is Big Iron UNIX Computer?“. *nixCraft*. 18.11.2008. Internet. 30.9.2014. <<http://www.cyberciti.biz/faq/bigiron-unix-systems/>>
- „What is DS3/T3 and E3 and what are the differences between T3/DS3 and E3?“. *AD-net Technology CO*. n.d. Internet. 30.9.2014. <<http://www.ad-net.com.tw/index.php?id=499>>
- „What is FPS (Frames Per Second)?“. *SecurityCameraKing.com*. Techpro Security Products LLC. 22.3.2010. Internet. 29.9.2014. <<http://www.securitycameraking.com/securityinfo/what-is-fps-frames-per-second/>>
- „What is Pro Tools – Mbox?“. *Avid Technology*. n.d. Internet. 30.9.2014. <<http://www.avid.com/US/products/mbox>>
- „What is SSL?“. *GMO GlobalSign*. n.d. Internet. 30.9.2014. <<https://www.globalsign.eu/ssl-information-center/what-is-ssl.html>>

- „What is the difference between an absolute and a relative URL?“. *Indiana University*. The Trustees of Indiana University. 19.3.2013. Internet. 29.9.2014. <<https://kb.iu.edu/d/abwp>>
- „What is YouTube?“. *Digital Unite*. n.d. Internet. 29.9.2014. <<http://digitalunite.com/guides/tv-video/what-youtube>>
- „What is Windows Media Player?“. *Digiarty Software*. n.d. Internet. 29.9.2014. <<http://www.winxdvd.com/resource/windows-media-player.htm>>
- „Who Was Charles Babbage?“. *Charles Babbage Institute*. University of Minnesota. 3.4.2013. Internet. 30.9.2014. <<http://www.cbi.umn.edu/about/babbage.html>>
- „wikiHow to Use Google Alerts“. *wikiHow*. 24.9.2014. Internet. 29.9.2014. <<http://www.wikihow.com/Use-Google-Alerts>>
- „William Gibson“. EMP Museum. n.d. Internet. 30.9.2014. <<http://web.archive.org/web/20120722083618/http://www.empmuseum.org/exhibitions/ind ex.asp?articleID=1282>>
- „Win32/Hydra“. *Eset*. n.d. Internet. 30.9.2014. <<http://www.eset.com/us/threat-center/encyclopedia/threats/hydra/>>
- „Wolfenstein 3D“. *Wikia Inc.* n.d. Internet. 29.9.2014. <http://wolfenstein.wikia.com/wiki/Wolfenstein_3D>
- „Wolfenstein 3D source code“. *Wikia inc.* n.d. Internet. 29.9.2014. <http://wolfenstein.wikia.com/wiki/Wolfenstein_3D_source_code>
- „Wolfenstein 3D [Mac]“. *Theodor Lauppert's Website*. 28.8.2008. Internet. 29.9.2014. <<http://theodor.lauppert.ws/games/wolfmac.htm>>
- „2600 Magazine“. <http://www.2600.com/>
- „2600 Magazine: The Hacker Quarterly“. *Barnesandnoble.com*. n.d. Internet. 30.9.2014. <<http://www.barnesandnoble.com/w/2600-magazine-2600-magazine/1115893352?ean=2940016773599>>
- Alderman, Nathan. „Safari 6 a slight but sleek upgrade for Apple's browser“. *Macworld*. IDG Consumer & SMB. 9.8.2012. Internet. 29.9.2014. <http://www.macworld.com/article/1168043/safari_6_a_slight_but_sleek_upgrade_for_apple_s_browser.html>
- Aarti, R. „Broadband Vs. Dial-Up Connection“. *Buzzle.com*. 23.6.2009. Internet. 30.9.2014. <<http://www.buzzle.com/articles/broadband-vs-dial-up-connection.html>>
- Birch, David G.W., i S. Peter Buck. „What is Cyberspace?“. *Hyperion 1*. n.d. Internet. 30.9.2014. <http://www.nadir.org/nadir/archiv/Kultur/CyberPunk/whatis_cyberspace.article.html>

- Bonsor, Kevin, i Ryan Johnson. „How Facial Recognition Systems Work“. *HowStuffWorks*. InfoSpace LLC. 4.9.2001. Internet. 29.9.2014.
<<http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm>>
- Boswell, Wendy. „MSN Search“. *About.com*. IAC. n.d. Internet. 29.9.2014.
<http://websearch.about.com/od/enginesanddirectories/a/msn_search.htm>
- Bradley, Tony. „What Is A Bot?“. *About.com*. IAC. n.d. Internet. 30.9.2014.
<http://netsecurity.about.com/od/frequentlyaskedquestions/qt/pr_bot.htm>
- Carter, Adam. „Why is security camera video still so terrible?“. *CBC*. 20.2.2014. Internet. 29.9.2014. <<http://www.cbc.ca/news/canada/hamilton/news/why-is-security-camera-video-still-so-terrible-1.2542359>>
- Davendranath G. Jha. *Computer Worms and Viruses*. „Computer Concepts and Management Information Systems“. str. 70. Asoke K. Ghosh, Delhi. 3.2013. Internet. 30.9.2014.
<<http://books.google.hr/books?id=YcMDLF7xETIC&printsec=frontcover#v=onepage&q&f=false>>
- Davis, Kai. „Viruses: A History“. *ParetoLogic*. 9.2008. Internet. 30.9.2014.
<http://www.paretologic.com/resources/newsletter/viruses_a_history.aspx>
- Drisko, James. „Transcribing via computer“. *Social Work Resources*. 23.10.2007. Internet. 30.9.2014. <<http://sophia.smith.edu/~jdrisko/transcription.htm>>
- Evers, Joris. „Opera preview puts widgets on stage“. *CNET*. CBS Interactive Inc. 5.2.2006. Internet. 29.9.2014. <http://news.cnet.com/Opera-preview-puts-widgets-on-stage/2100-1032_3-6035227.html>
- Fitzpatrick, Laura. „A Different Kind of Cookie Monster“. *Time Inc*. 8.9.2008. Internet. 30.9.2014.
<http://content.time.com/time/specials/packages/article/0,28804,1839579_1839578_1839526,00.html>
- Garmon, Jay. „Geek Trivia: Search party of the second part“. *TechRepublic*. CBS Interactive. 16.3.2009. Internet. 29.9.2014.
<<http://www.techrepublic.com/blog/geekend/geek-trivia-search-party-of-the-second-part/2/>>
- Gillette, Felix. „The Rise and Inglorious Fall of Myspace“. *Businessweek.com*. Bloomberg L.P. 22.6.2011. Internet. 29.9.2014.
<http://www.businessweek.com/magazine/content/11_27/b4235053917570.htm>
- Go, Hermelito. „What does fork() do?“. *UnixGuide.net*. n.d. Internet. 30.9.2014.
<<http://www.unixguide.net/unix/programming/1.1.1.shtml>>
- Grabianowski, Ed, i Stephanie Crawford. „How PayPal Works“. *HowStuffWorks*. InfoSpace LLC. 13.12.2005. Internet. 29.9.2014.
<<http://money.howstuffworks.com/paypal.htm>>

- Grant, Ash. „Top 10 Infamous Hackers“. *Toptenz.net*. 24.5.2010. Internet. 30.9.2014. <<http://www.toptenz.net/top-10-infamous-hackers.php>>
- Grimmick, Robert. „What Is Disk Cloning?“. *WiseGEEK.org*. Conjecture Corporation. 28.9.2014. Internet. 30.9.2014. <<http://www.wisegeek.com/what-is-disk-cloning.htm>>
- Hannibal. „RISC vs. CISC: the Post-RISC Era“. *ArsTechnica.com*. n.d. Internet. 30.9.2014. <<http://archive.arstechnica.com/cpu/4q99/risc-cisc/rvc-6.html>>
- Jeff. „Guess why we're moving to 256-bit AES keys“. *AgileBits Inc.* 9.3.2013. Internet. 30.9.2014. <<http://blog.agilebits.com/2013/03/09/guess-why-were-moving-to-256-bit-aes-keys/>>
- Karbo, Michael B. „Chip sets for Intel's P6 processors“. *Karbosguide.com*. n.d. Internet. 30.9.2014. <<http://www.karbosguide.com/hardware/module2d04.htm>>
- Karch, Marziah. „What is Google?“. *About.com*. IAC. n.d. Internet. 29.9.2014. <<http://google.about.com/od/googlebasics/p/whatisgoogle.htm>>
- Kayne, R. „What Is a Modem?“. *WiseGEEK.org*. Conjecture Corporation. 26.9.2014. Internet. 30.9.2014. <<http://www.wisegeek.org/what-is-a-modem.htm>>
- Kelly, Samantha M. „The 30 Most Popular Passwords Stolen From LinkedIn“. *Mashable*. 9.6.2012. Internet. 30.9.2014. <<http://mashable.com/2012/06/08/linkedin-stolen-passwords-list/>>
- Kershner, Kate. „What are supercomputers currently used for?“. *HowStuffWorks*. InfoSpace LLC. 4.9.2012. Internet. 30.9.2014. <<http://computer.howstuffworks.com/supercomputers-used-for.htm>>
- Kissell, Joe. „Are Your Passwords Safe?“. *Macworld*. 30. Svezak. 3. br. 3.2013. EBSCOhost. Internet. 30.9.2014.
- Lemm, Michael. „What's the Difference Between DS3 and T3 Bandwidth?“. *EzineArticles.com*. SparkNET. 9.11.2005. Internet. 30.9.2014. <<http://ezinearticles.com/?Whats-the-Difference-Between-DS3-and-T3-Bandwidth?&id=94209>>
- Logik Bomb. „Hacker's Encyclopedia“. V2.5. 1997. Internet. 30.9.2014. <<http://insecure.org/stf/hackenc.txt>>
- McClelland, Deke, i Colleen Wheeler. „Healing a Damaged Image“. *Photoshop Elements 8 One-on-One*. Str. 132. <<http://books.google.hr/books?id=HZH0AQkh8uYC&printsec=frontcover#v=onepage&q&f=false>>
- McMahon, Mary. „What is a Supercomputer?“. *WiseGEEK.org*. Conjecture Corporation. 14.9.2014. Internet. 30.9.2014. <<http://www.wisegeek.org/what-is-a-supercomputer.htm>>
- Mitchell, Bradley. „Modems, V.92, and You“. *About.com*. n.d. Internet. 30.9.2014. <<http://compnetworking.about.com/library/weekly/aa112100a.htm>>

- Mitchell, Bradley. „Sniffer“. *About.com*. n.d. Internet. 30.9.2014.
<http://compnetworking.about.com/od/networksecurityprivacy/g/bldef_sniffer.htm>
- Mitchell, Bradley. „Ways You Can Hide Your Public IP Address“. *About.com*. IAC. n.d. Internet. 29.9.2014.
<<http://compnetworking.about.com/od/workingwithipaddresses/f/hideipaddress.htm>>
- Mueller, Scott. „Intel P6 (686) Sixth-Generation Processors“. *Que Publishing*. Pearson Education. 21.7.2006. Internet. 30.9.2014.
<<http://www.quepublishing.com/articles/article.aspx?p=482324&seqNum=17>>
- Ngak, Chenda. „The 25 most common passwords in 2013“. *CBS News*. 21.1.2014. Internet. 30.9.2014. <<http://www.cbsnews.com/news/the-25-most-common-passwords-of-2013/>>
- Nicol, David M. „Hacking the Lights Out“. *Scientific American*. 305. svezak. br.1. 7.2011. EBSCOhost. Internet. 30.9.2014.
- Northcutt, Stephen. „Logic Bombs, Trojan Horses, and Trap Doors“. *SANS Technology Institute*. n.d. Internet. 30.9.2014. <<http://www.sans.edu/research/security-laboratory/article/log-bmb-trp-door>>
- Parks, Aaron. „Hackers & Hackers: Fact Versus Film in the Context of Compromising Computer Systems“. 2010. Str. 13.
- Paskin, Willa i Laura Reineke. „Bockmail, Roundsearch, and Other Websites TV Made Up This Year“. *Vulture.com*. New York Media LLC. 22.12.2011. Internet. 29.9.2014.
<<http://www.vulture.com/2011/12/websites-tv-made-up-this-year.html>>
- Queen, Jacob. „What Is Data Corruption?“. *WiseGEEK.org*. Conjecture Corporation. 29.9.2014. Internet. 30.9.2014. <<http://www.wisageek.com/what-is-data-corruption.htm>>
- Rankin, Bob. „What Is Bing?“. *AskBobRankin.com*. Bob Rankin. 2.6.2009. Internet. 29.9.2014. <http://askbobrankin.com/what_is_bing.html>
- Ranum, Marcus J. „One-Time-Pad (Vernam's Cipher)“. n.d. Internet. 30.9.2014.
<http://www.ranum.com/security/computer_security/papers/otp-faq/>
- Roos, Dave. „How Pro Tools Software and Hardware Works“. *HowStuffWorks*. InfoSpace LLC. 25.7.2008. Internet. 30.9.2014. <<http://entertainment.howstuffworks.com/pro-tools-software-hardware.htm>>
- Rouse, Margaret. „Botnet (zombie army)“. *SearchSecurity.com*. TechTarget. 2.2012. Internet. 30.9.2014. <<http://searchsecurity.techtarget.com/definition/botnet>>
- Rouse, Margaret. „Computer Fraud and Abuse Act (CFAA)“. *SearchCompliance.com*. TechTarget. 6.2012. Internet. 30.9.2014.
<<http://searchcompliance.techtarget.com/definition/The-Computer-Fraud-and-Abuse-Act-CFAA>>

- Rouse, Margaret. „Face recognition“. *WhatIs.com*. TechTarget. 2.2012. Internet. 29.9.2014. <<http://whatis.techtarget.com/definition/facial-recognition>>
- Rouse, Margaret. „Facebook“. *WhatIs.com*. TechTarget. 8.2014. Internet. 29.9.2014. <<http://whatis.techtarget.com/definition/Facebook>>
- Rouse, Margaret. „Mainframe (big iron)“. *SearchDataCenter.com*. TechTarget. 9.2005. Internet. 30.9.2014. <<http://searchdatacenter.techtarget.com/definition/mainframe>>
- Rouse, Margaret. „Motion gaming (motion-controlled gaming)“. *WhatIs.com*. TechTarget. 6.2011. Internet. 29.9.2014. <<http://whatis.techtarget.com/definition/motion-gaming-motion-controlled-gaming>>
- Rouse, Margaret. „Network Address Translation (NAT)“. *SearchEnterpriseWAN.com*. TechTarget. 4.2007. Internet. 29.9.2014. <<http://searchenterprisewan.techtarget.com/definition/Network-Address-Translation>>
- Rouse, Margaret. „Source code“. *SearchSOA.com*. TechTarget. 9.2005. Internet. 29.9.2014. <<http://searchsoa.techtarget.com/definition/source-code>>
- Rouse, Margaret. „Subnet (subnetwork)“. *SearchNetworking.com*. TechTarget. 3.2007. Internet. 29.9.2014. <<http://searchnetworking.techtarget.com/definition/subnet>>
- Rouse, Margaret. „Supercomputer“. *WhatIs.com*. TechTarget. 9.2008. Internet. 30.9.2014. <<http://whatis.techtarget.com/definition/supercomputer>>
- Rouse, Margaret. „Thin-film transistor (TFT)“. *WhatIs.com*. TechTarget. 9.2005. Internet. 30.9.2014. <<http://whatis.techtarget.com/definition/thin-film-transistor-TFT>>
- Rouse, Margaret. „Wikipedia“. *WhatIs.com*. TechTarget. 1.2008. Internet. 29.9.2014. <<http://whatis.techtarget.com/definition/Wikipedia>>
- Schindler, Laura. „Web-Based Education: A Speech Recognition and Synthesis Tool“. Stetson University. DeLand, Florida. 2005. Internet. 29.9.2014. <<http://www2.stetson.edu/~helaarag/Laura-proposal.pdf>>
- Schwabe, Peter. „Security Issues in Cloud Computing“. 14.10.2011. Str. 1. Internet. 30.9.2014. <<http://cryptojedi.org/peter/data/notes-20111014.pdf>>
- Sharma, F. Reena, i S. Geetanjali Wasson. „Speech Recognition and Synthesis Tool: Assistive Technology for Physically Disabled Persons“. *International Journal of Computer Science and Telecommunications*, 3. svezak, 4. br., 4.2012. Internet. 29.9.2014. <http://www.ijcst.org/Volume3/Issue4/p17_3_4.pdf>
- Siciliano, Robert. „What is a Keylogger?“. *Mcafee.com*. 23.7.2013. Internet. 30.9.2014. <<http://blogs.mcafee.com/consumer/what-is-a-keylogger>>
- Strickland, Jonathan. „How Cloud Computing Works“. *HowStuffWorks*. InfoSpace LLC. 8.4.2008. Internet. 29.9.2014. <<http://computer.howstuffworks.com/cloud-computing/cloud-computing.htm>>

- Strickland, Jonathan. „How Craigslist Works“. *HowStuffWorks*. InfoSpace LLC. 1.11.2007. Internet. 29.9.2014. <<http://money.howstuffworks.com/craigslist.htm>>
- Strickland, Jonathan. „How Zombie Computers Work“. *HowStuffWorks*. InfoSpace LLC. 10.9.2007. Internet. 30.9.2014. <<http://computer.howstuffworks.com/zombie-computer1.htm>>
- Tanase, Matthew. „Sniffers: What They Are and How to Protect Yourself“. *Symantec Corporation*. 3.11.2010. Internet. 30.9.2014. <<http://www.symantec.com/connect/articles/sniffers-what-they-are-and-how-protect-yourself>>
- Tavares, C.D. „Origin of the Cookie Monster“. 13.3.1995. *Multicians*. Internet. 30.9.2014. <<http://www.multicians.org/cookie.html>>
- The Mentor. „The Conscience of a Hacker“. *Phrack Magazine*. 8.1.1986. Internet. 30.9.2014. <<http://phrack.org/issues/7/3.html>>
- Tyson, Jeff. „How LCDs Work“. *HowStuffWorks*. InfoSpace LLC. 17.7.2000. Internet. 30.9.2014. <<http://electronics.howstuffworks.com/lcd4.htm>>
- Villasenor, John. „The Hacker in Your Hardware“. *Scientific American*. 303. svezak. Br.2. 8.2010. EBSCOhost. Internet. 30.9.2014.
- Wentworth, Rob. „Computer Virus!“. 7.1996. *The Digital Viking*. Internet. 30.9.2014. <<http://uanr.com/articles/virus.html>>
- Zeevi, Daniel. „Twitter 101: What is Twitter Really About?“. *SocialMediaToday.com*. 12.4.2013. Internet. 29.9.2014. <<http://socialmediatoday.com/daniel-zeevi/1371811/twitter-101-what-twitter-really-about>>

MATERIJALI

- *Broadchurch*: ep. 101. *ITV*. 4.3.2013. Televizija.
- *Broadchurch*: ep. 108. *ITV*. 22.4.2013. Televizija.
- *Brooklyn Nine-Nine*: ep. 110 („Thanksgiving“). *Fox*. 26.11.2013. Televizija.
- *Brooklyn Nine-Nine*: ep. 114 („The Ebony Falcon“). *Fox*. 21.1.2014. Televizija.
- *Casino Royale*. Red. Martin Campbell. Glum. Daniel Craig. *Metro-Goldwyn-Mayer, Columbia Pictures*. 2006. Film.
- *CSI: NY*: ep. 110 („Night, Mother“). *CBS*. 15.12.2004. Televizija
- Čudesni Spider-Man. Red. Marc Webb. Glum. Andrew Garfield. *Sony Pictures Entertainment*. 2012. Film.
- Doktor Who: ep. 101 („Rose“). *BBC One*. 26.3.2005. Televizija.
- Doktor Who: ep. 106 („Dalek“). *BBC One*. 30.4.2005. Televizija.
- Hakeri. Red. Iain Softley. Glum. Jonny Lee Miller. *United Artists*. 1995. Film.
- Izvorni kod. Red. Duncan Jones. Glum. Jake Gyllenhaal. *Summit Entertainment*. 2011. Film.
- Jekyll: ep. 106 („Episode Six“). *BBC One*. 28.7.2007. Televizija.
- *Kick-Ass 2*. Red. Jeff Wadlow. *Universal Pictures*, 2013. Film.
- Luther: ep. 104 („Episode 4“). *BBC One*. 25.5.2010. Televizija.
- Luther: ep. 203 („Episode 3“). *BBC One*. 28.6.2011. Televizija
- Luther: ep. 204 („Episode 4“). *BBC One*. 5.7.2011. Televizija.
- *Mreža*. Red. Irwin Winkler. Glum. Sandra Bullock. *Columbia Pictures*. 1995. Film.
- Obavještajci: ep. 203 („Spiders“). *BBC Three*. 9.6.2003. Televizija
- Obavještajci: ep. 307 („Outsiders“). *BBC Three*. 20.11.2004. Televizija.
- Obavještajci: ep. 405 („The Book“). *BBC One*. 6.10.2005. Televizija.
- Obavještajci: ep. 409 („The Sting“). *BBC One*. 3.11.2005. Televizija.
- Obavještajci: ep. 410 („Diana“). *BBC One*. 10.11.2005. Televizija.
- Ona. Red. Spike Jonze. Glum. Joaquin Phoenix. *Warner Bros. Pictures*. 2013. Film.
- Operacija *Swordfish*. Red. Dominic Sena. *Warner Bros. Pictures*. 2001. Film.

- *Parks and Recreation*: ep. 605 („Gin It Up!“). *NBC*. 17.10.2013. Televizija.
- Put prema dolje: ep. 102 („Cat's in the Bag...“). *AMC*. 27.1.2008. Televizija.
- Put prema dolje: ep. 212 („Phoenix“). *AMC*. 24.5.2009. Televizija.
- Put prema dolje: ep. 312 („Half Measures“). *AMC*. 6.6.2010. Televizija
- Put prema dolje: ep. 402 („Thirty-Eight Snub“). *AMC*. 24.7.2011. Televizija.
- Put prema dolje: ep. 501 („Live Free or Die“). *AMC*. 15.7.2012. Televizija.
- Put prema dolje: ep. 515 („Granite State“). *AMC*. 22.9.2013. Televizija.
- Sinovi anarhije: ep. 106 („AK-51“). *FX*. 8.10.2008. Televizija.
- Sinovi anarhije: ep. 205 („Smite“). *FX*. 6.10.2009. Televizija.
- Sinovi anarhije: ep. 210 („Balm“). *FX*. 10.11.2009. Televizija.
- Sinovi anarhije: ep. 505 („Orca Shrugged“). *FX*. 9.10.2012. Televizija.
- *Skyfall*. Red. Sam Mendes. Glum. Daniel Craig. *Metro-Goldwyn-Mayer, Columbia Pictures*. 2012. Film.
- Ubi me dosada: ep. 101 („Stockholm Syndrome“). *HBO*. 20.9.2009. Televizija.
- Žica: ep. 205 („Undertow“). *HBO*. 29.6.2003. Televizija.
- Žica: ep. 206 („All Prologue“). *HBO*. 6.7.2003. Televizija.
- Žica: ep. 209 („Stray Rounds“). *HBO*. 3.8.2003. Televizija.